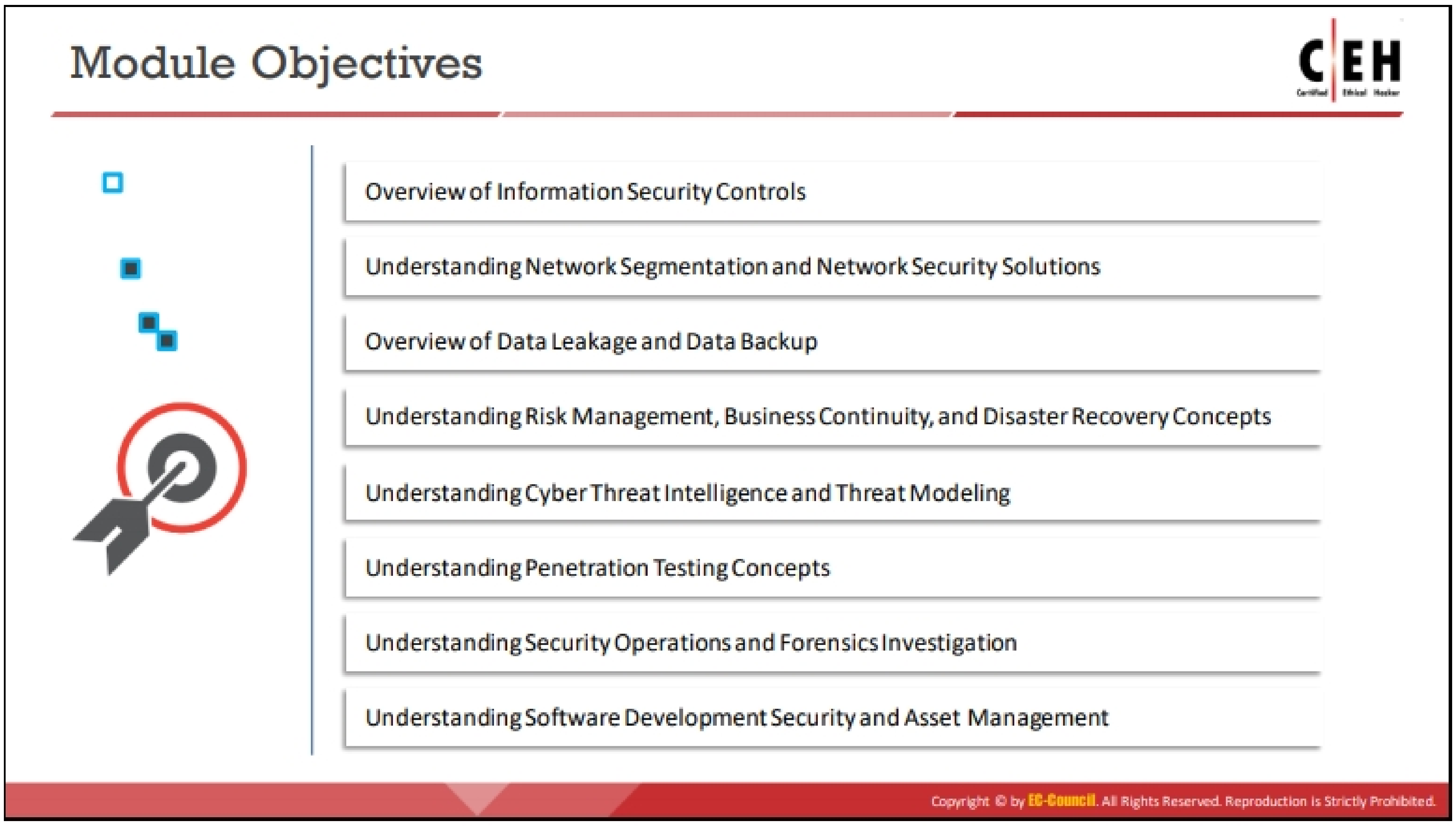
C|EH™

Certified Ethical Hacker

Appendix B:

Ethical Hacking Essential Concepts - II



Module Objectives

- Overview of Information Security Controls
- Understanding Network Segmentation and Network Security Solutions
- Overview of Data Leakage and Data Backup
- Understanding Risk Management, Business Continuity, and Disaster Recovery Concepts
- Understanding Cyber Threat Intelligence and Threat Modeling
- Understanding Penetration Testing Concepts
- Understanding Security Operations and Forensics Investigation
- Understanding Software Development Security and Asset Management

Information Security Controls

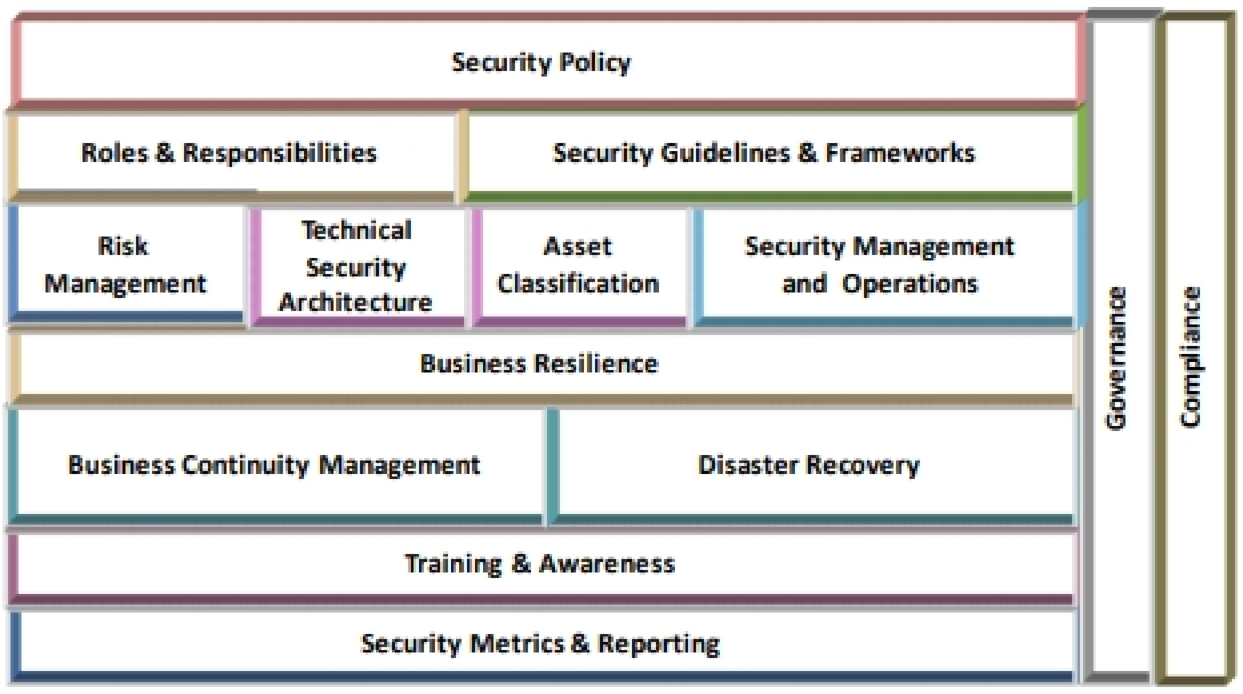
Notes:

Information Security Management Program

- Programs that are designed to **enable a business to operate in a state of reduced risk**
- Encompasses all **organizational** and **operational processes**, and participants relevant to information security

Information Security Management Framework

A combination of **well-defined** policies, processes, procedures, standards, and guidelines to establish the required **level of information security**


Security Policy
Roles & Responsibilities
Security Guidelines & Frameworks
Risk Management
Technical Security Architecture
Asset Classification
Security Management and Operations
Business Resilience
Business Continuity Management
Disaster Recovery
Training & Awareness
Security Metrics & Reporting
Governance
Compliance

Enterprise Information Security Architecture (EISA)

- EISA is a set of requirements, processes, principles, and models that **determines the structure and behavior of an organization's information systems**

EISA Goals

1. **Helps to monitor and detect network behaviors** in real time, acting upon internal and externals security risks
2. Helps an organization **detect and recover from security breaches**
3. Helps to prioritize the resources of an organization and **monitor various threats**
4. **Benefits organization's budget in cost prospective** when incorporated in incident response, disaster recovery, event correlation, and other security provisions
5. Helps to analyze the procedure needed for the IT department to function properly and **identify assets**
6. **Helps to perform risk assessment** of an organization's IT assets with the cooperation of IT staff

Notes: ____

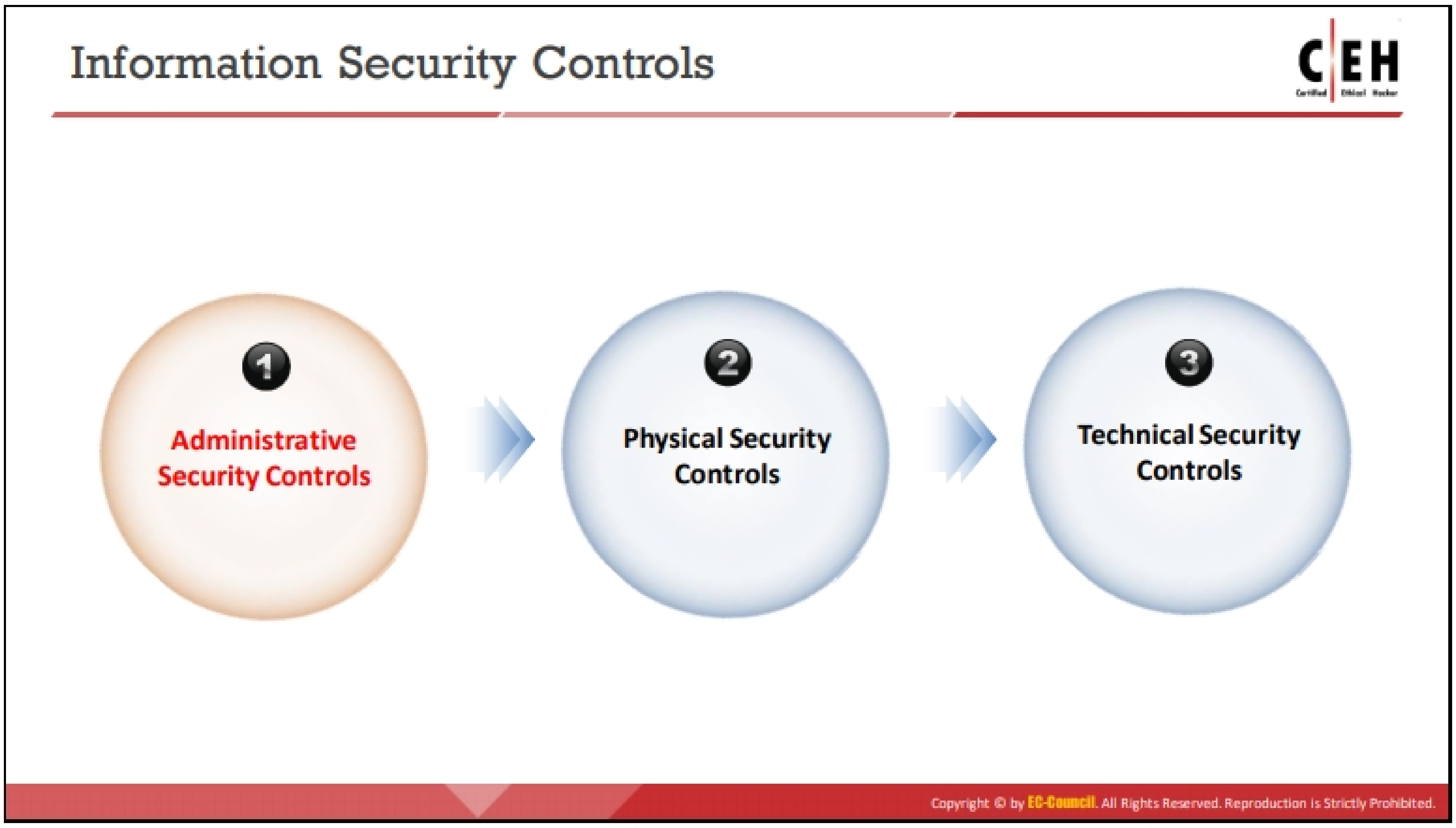
____

____

____

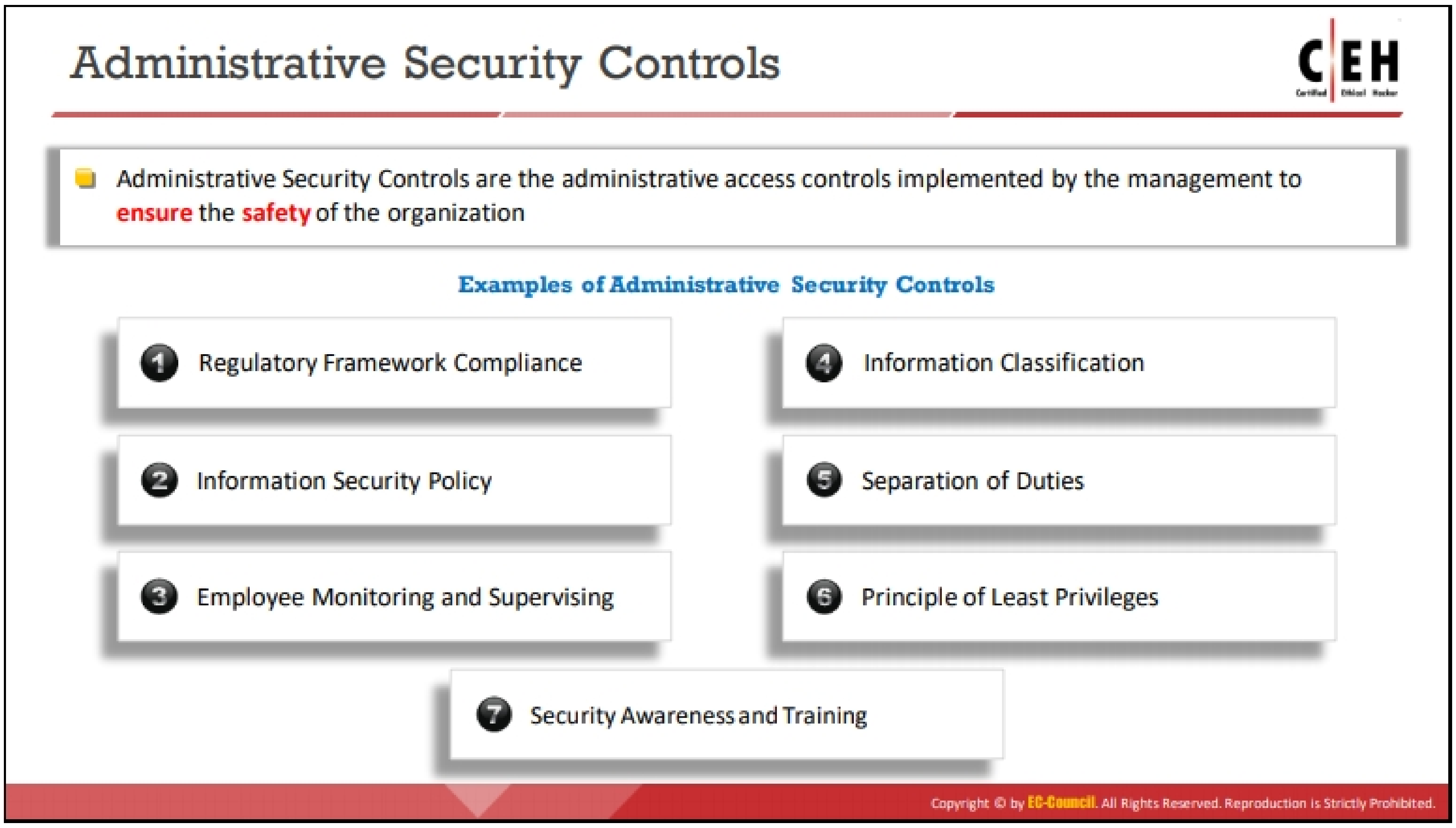
____

____



Information Security Controls

1. Administrative Security Controls
2. Physical Security Controls
3. Technical Security Controls



Administrative Security Controls

- Administrative Security Controls are the administrative access controls implemented by the management to **ensure** the **safety** of the organization

Examples of Administrative Security Controls

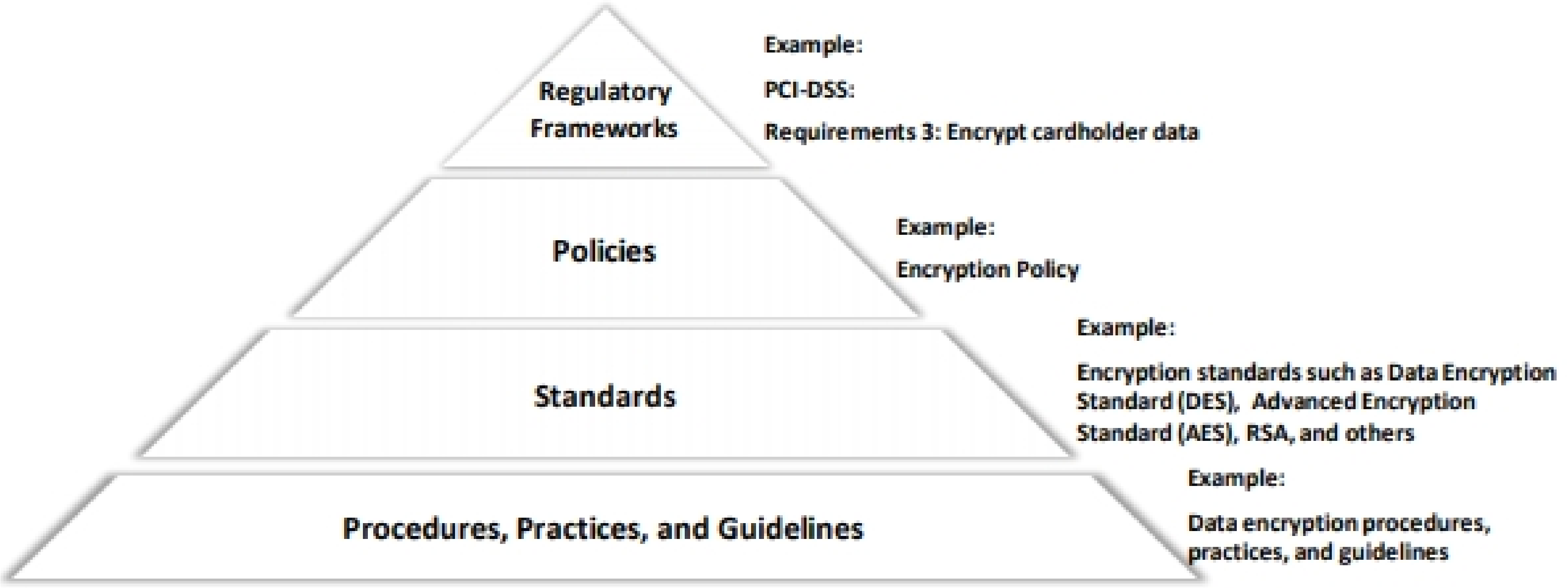
1. Regulatory Framework Compliance
2. Information Security Policy
3. Employee Monitoring and Supervising
4. Information Classification
5. Separation of Duties
6. Principle of Least Privileges
7. Security Awareness and Training

Notes: ____

Regulatory Frameworks Compliance

- Complying with regulatory frameworks is a **collaborative effort** between governments and private bodies to encourage voluntary **improvements** to cybersecurity

Role of regulatory frameworks compliance in an organization's administrative security



Regulatory Frameworks
Example:
PCI-DSS:
Requirements 3: Encrypt cardholder data

Policies
Example:
Encryption Policy

Standards
Example:
Encryption standards such as Data Encryption Standard (DES), Advanced Encryption Standard (AES), RSA, and others

Procedures, Practices, and Guidelines
Example:
Data encryption procedures, practices, and guidelines

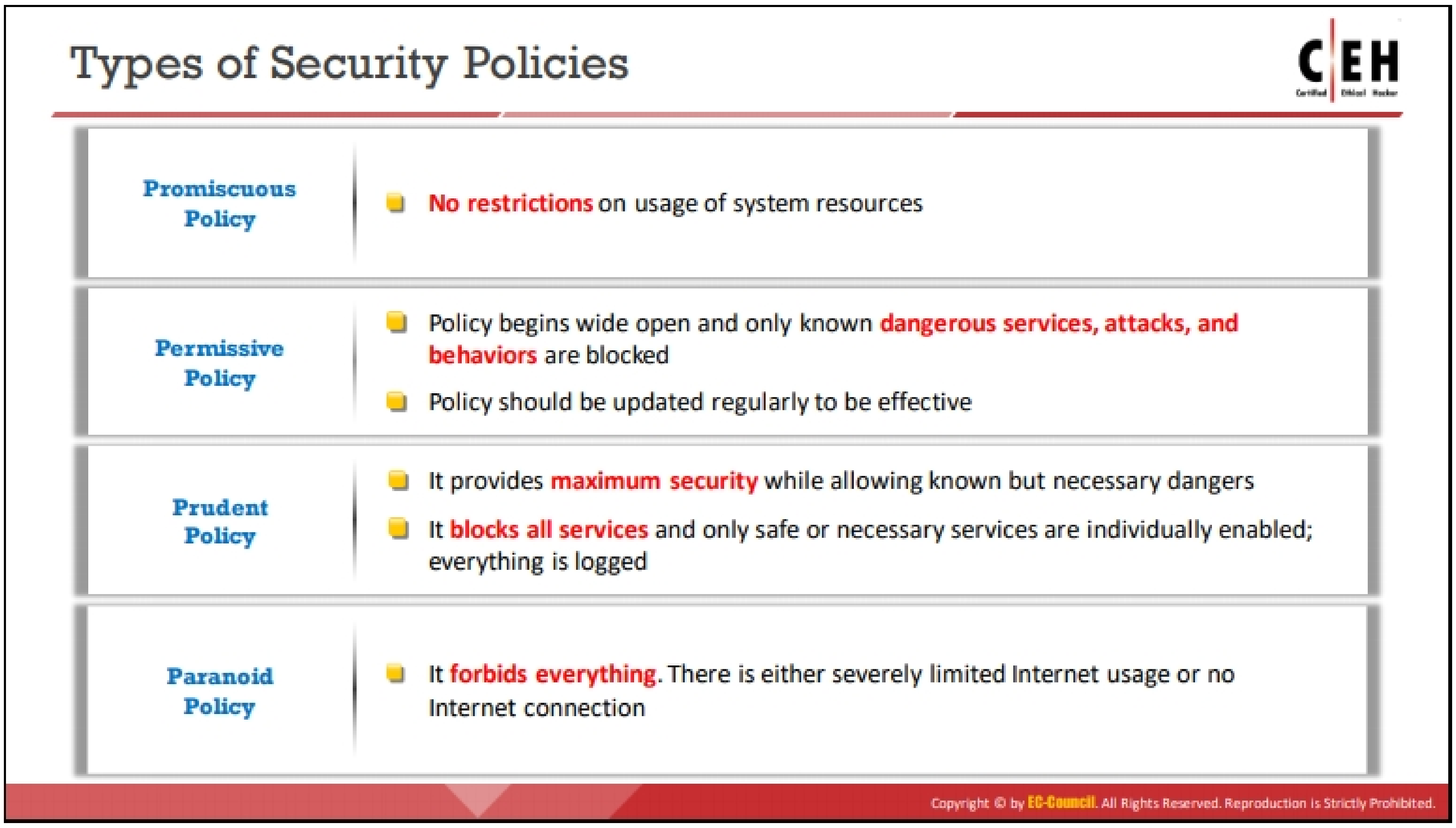
Information Security Policies

- Security policies are the foundation of **security infrastructure**
- Information security policy defines the basic security requirements and rules to be implemented in order to **protect** and **secure an organization's information systems**

Goals of Security Policies

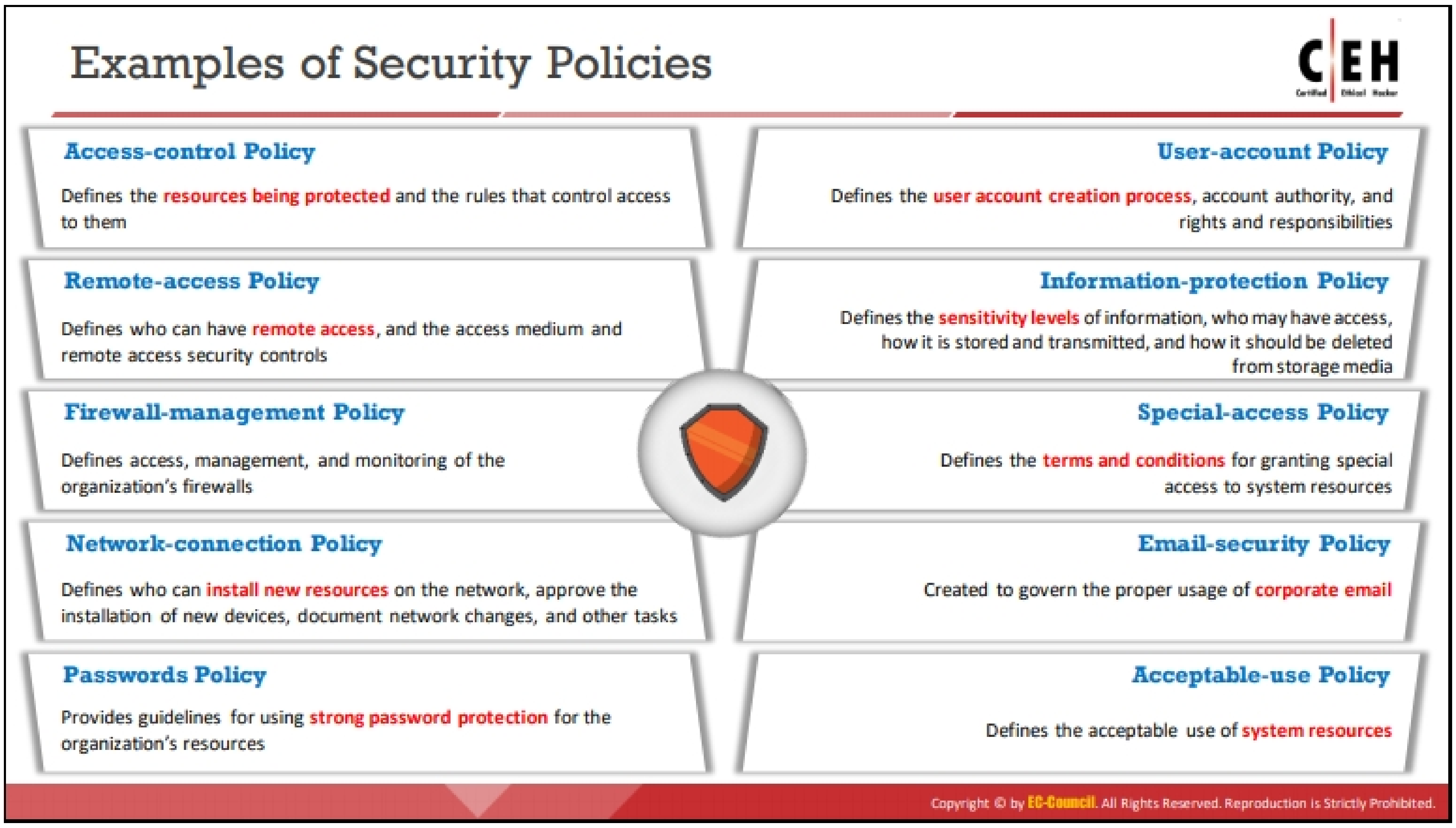
1. Maintain an outline for the management and administration of network security
2. Protect an organization's computing resources
3. Eliminate legal liabilities arising from employees or third parties
4. Prevent waste of the company's computing resources
5. Prevent unauthorized modifications of data
6. Reduce risks caused by illegal use of system resources
7. Differentiate the users' access rights
8. Protect confidential, proprietary information from theft, misuse, and unauthorized disclosure

Notes: ____



Types of Security Policies

Promiscuous Policy	No restrictions on usage of system resources
Permissive Policy	Policy begins wide open and only known dangerous services, attacks, and behaviors are blocked Policy should be updated regularly to be effective
Prudent Policy	It provides maximum security while allowing known but necessary dangers It blocks all services and only safe or necessary services are individually enabled; everything is logged
Paranoid Policy	It forbids everything. There is either severely limited Internet usage or no Internet connection



Examples of Security Policies

Access-control Policy

Defines the resources being protected and the rules that control access to them

Remote-access Policy

Defines who can have remote access, and the access medium and remote access security controls

Firewall-management Policy

Defines access, management, and monitoring of the organization's firewalls

Network-connection Policy

Defines who can install new resources on the network, approve the installation of new devices, document network changes, and other tasks

Passwords Policy

Provides guidelines for using strong password protection for the organization's resources

User-account Policy

Defines the user account creation process, account authority, and rights and responsibilities

Information-protection Policy

Defines the sensitivity levels of information, who may have access, how it is stored and transmitted, and how it should be deleted from storage media

Special-access Policy

Defines the terms and conditions for granting special access to system resources

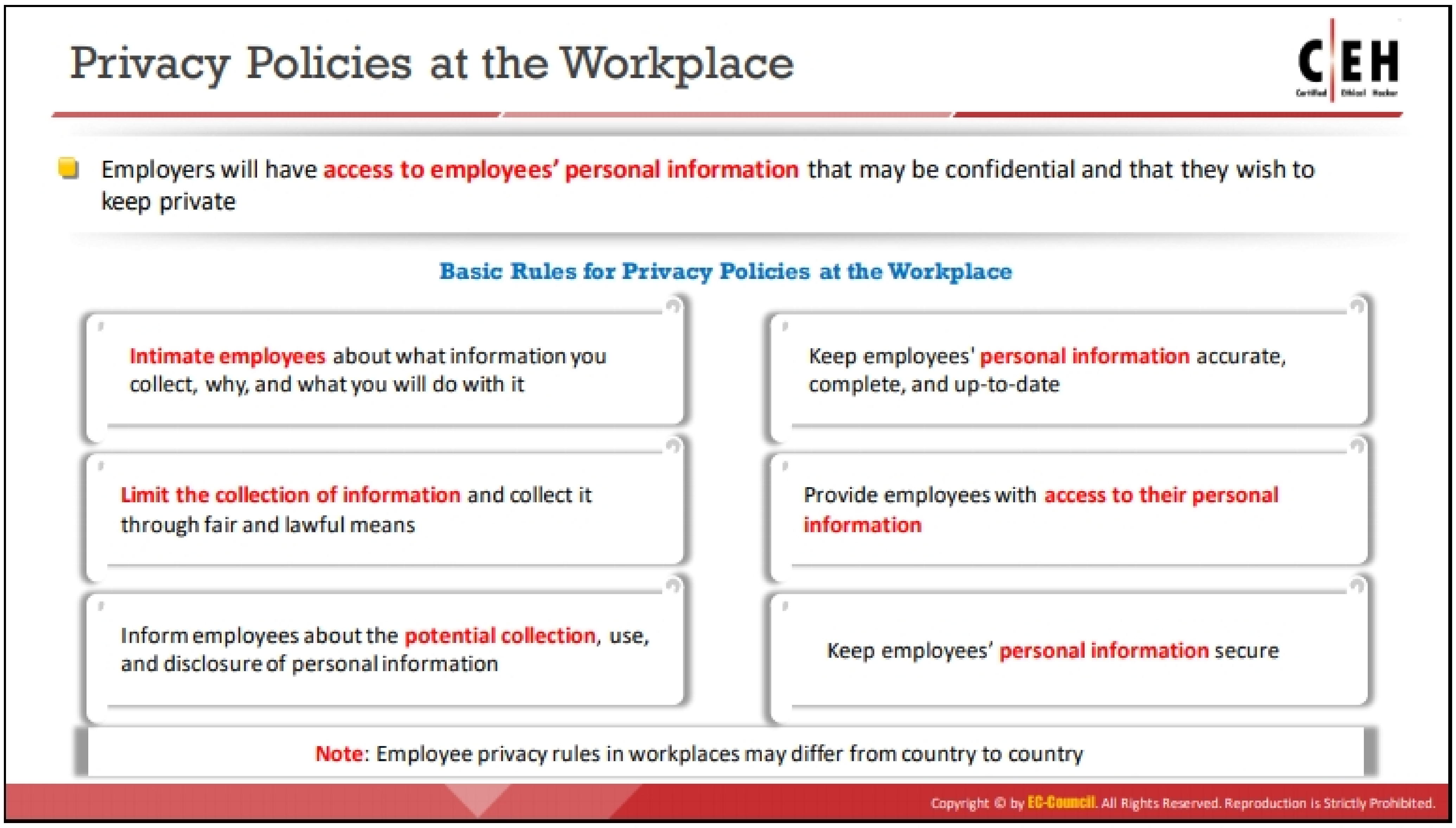
Email-security Policy

Created to govern the proper usage of corporate email

Acceptable-use Policy

Defines the acceptable use of system resources

Notes: ____



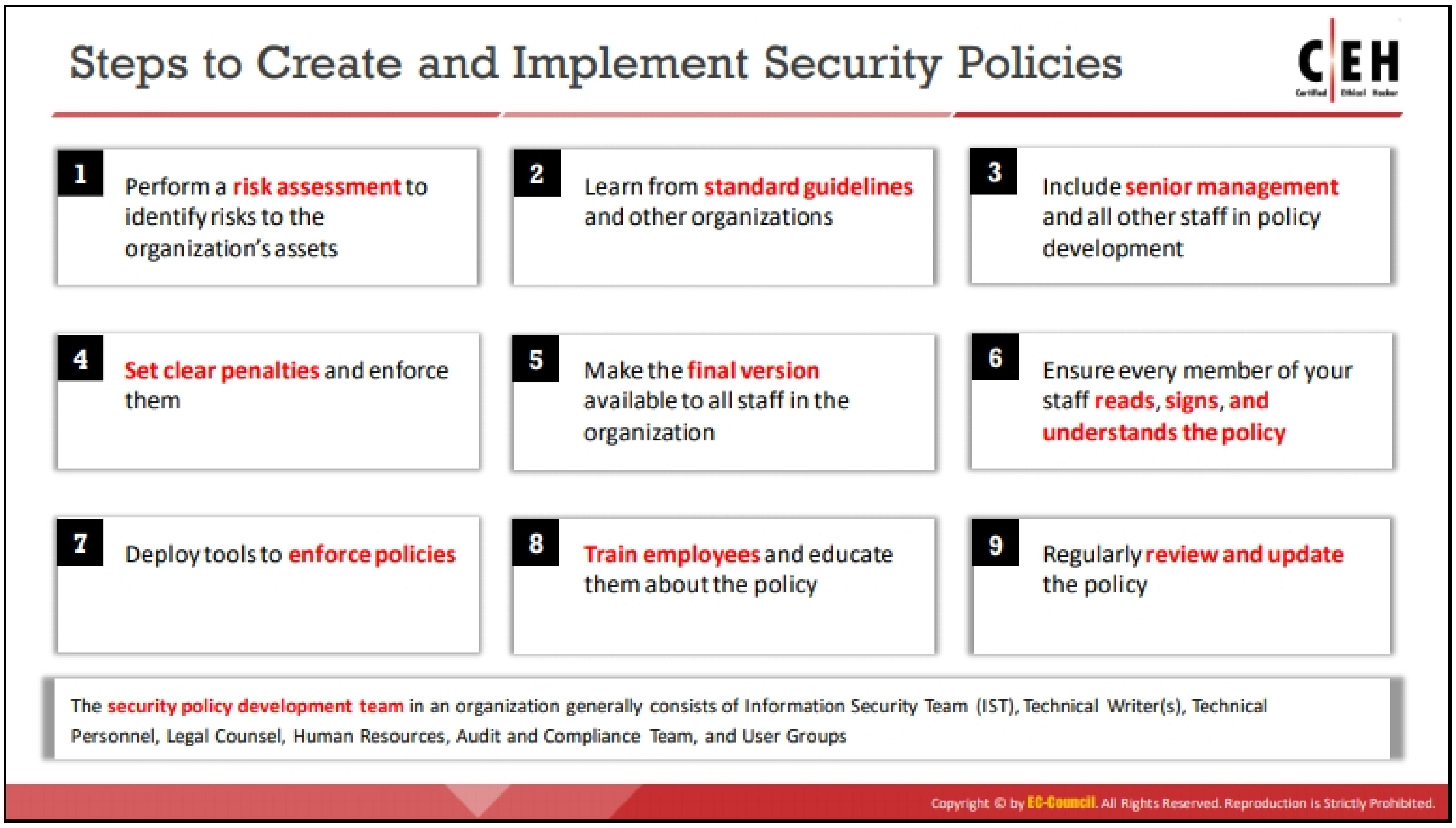
Privacy Policies at the Workplace

- Employers will have **access to employees' personal information** that may be confidential and that they wish to keep private

Basic Rules for Privacy Policies at the Workplace

- **Intimate employees** about what information you collect, why, and what you will do with it
- **Limit the collection of information** and collect it through fair and lawful means
- Inform employees about the **potential collection**, use, and disclosure of personal information
- Keep employees' **personal information** accurate, complete, and up-to-date
- Provide employees with **access to their personal information**
- Keep employees' **personal information** secure

Note: Employee privacy rules in workplaces may differ from country to country

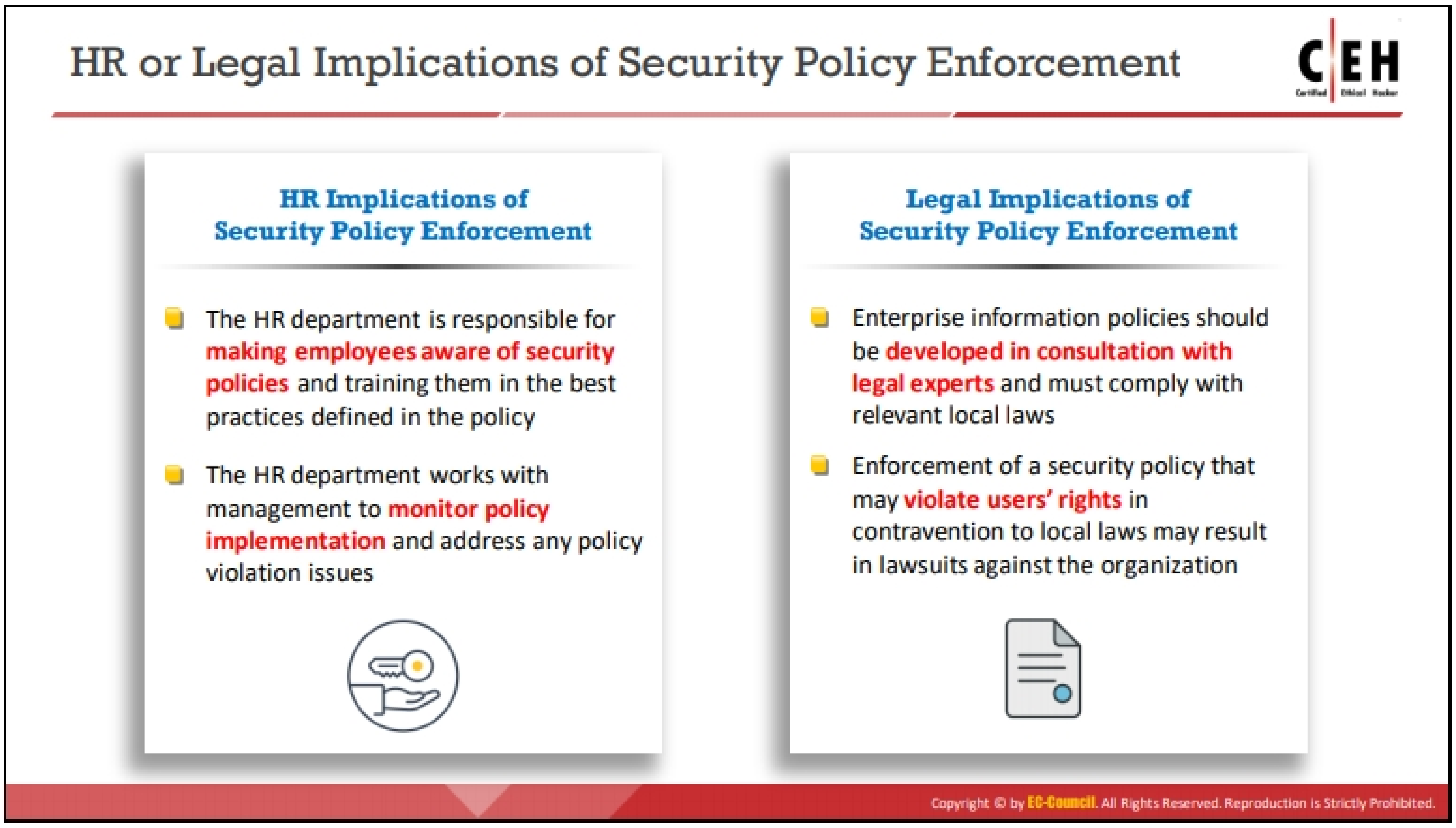


Steps to Create and Implement Security Policies

1. Perform a **risk assessment** to identify risks to the organization's assets
2. Learn from **standard guidelines** and other organizations
3. Include **senior management** and all other staff in policy development
4. **Set clear penalties** and enforce them
5. Make the **final version** available to all staff in the organization
6. Ensure every member of your staff **reads, signs, and understands the policy**
7. Deploy tools to **enforce policies**
8. **Train employees** and educate them about the policy
9. Regularly **review and update** the policy

The **security policy development team** in an organization generally consists of Information Security Team (IST), Technical Writer(s), Technical Personnel, Legal Counsel, Human Resources, Audit and Compliance Team, and User Groups

Notes:



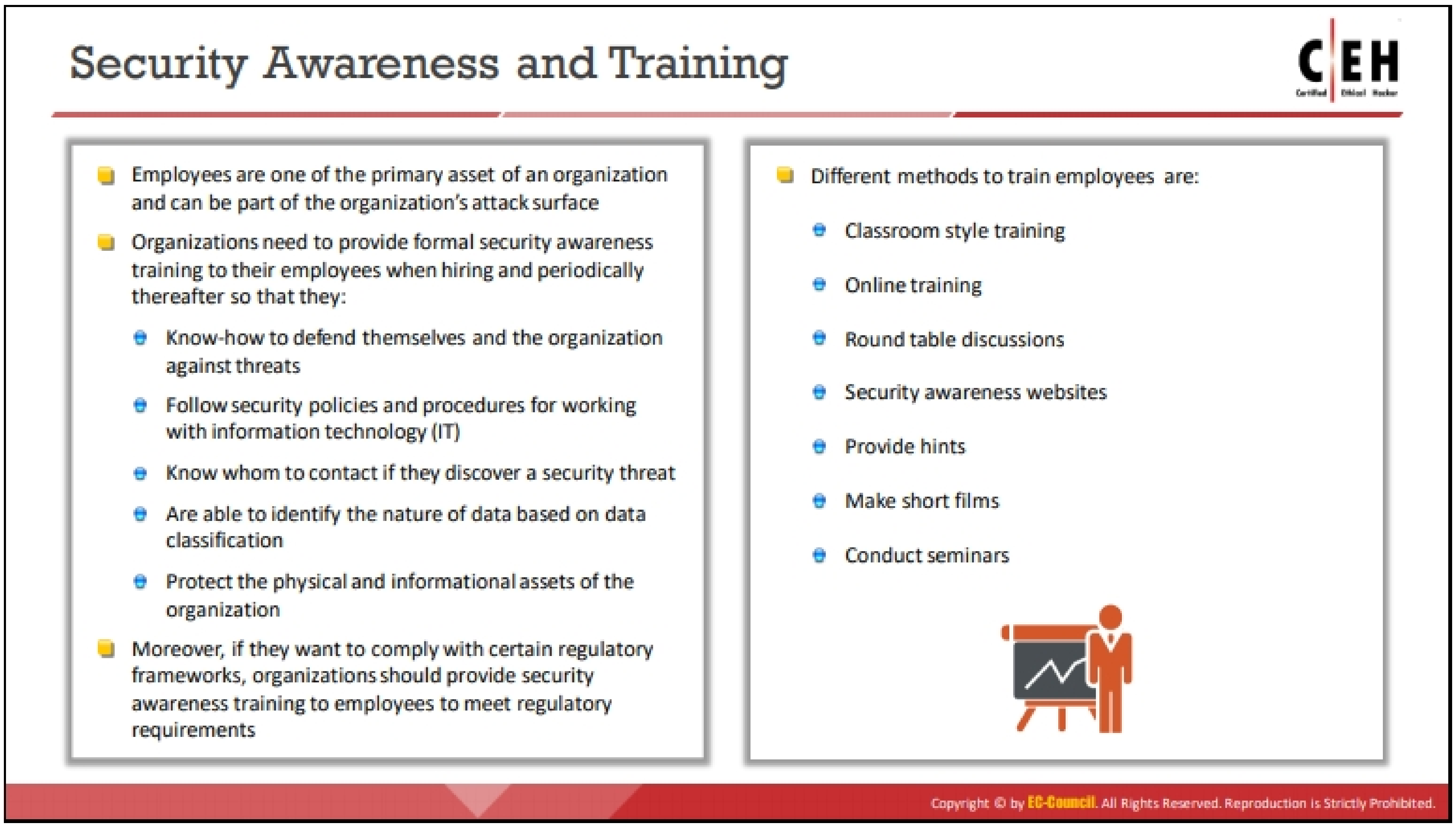
HR or Legal Implications of Security Policy Enforcement

HR Implications of Security Policy Enforcement

- The HR department is responsible for **making employees aware of security policies** and training them in the best practices defined in the policy
- The HR department works with management to **monitor policy implementation** and address any policy violation issues

Legal Implications of Security Policy Enforcement

- Enterprise information policies should be **developed in consultation with legal experts** and must comply with relevant local laws
- Enforcement of a security policy that may **violate users' rights** in contravention to local laws may result in lawsuits against the organization



Security Awareness and Training

- Employees are one of the primary asset of an organization and can be part of the organization's attack surface
- Organizations need to provide formal security awareness training to their employees when hiring and periodically thereafter so that they:
  - Know-how to defend themselves and the organization against threats
  - Follow security policies and procedures for working with information technology (IT)
  - Know whom to contact if they discover a security threat
  - Are able to identify the nature of data based on data classification
  - Protect the physical and informational assets of the organization
- Moreover, if they want to comply with certain regulatory frameworks, organizations should provide security awareness training to employees to meet regulatory requirements

- Different methods to train employees are:
  - Classroom style training
  - Online training
  - Round table discussions
  - Security awareness websites
  - Provide hints
  - Make short films
  - Conduct seminars

Notes: ____

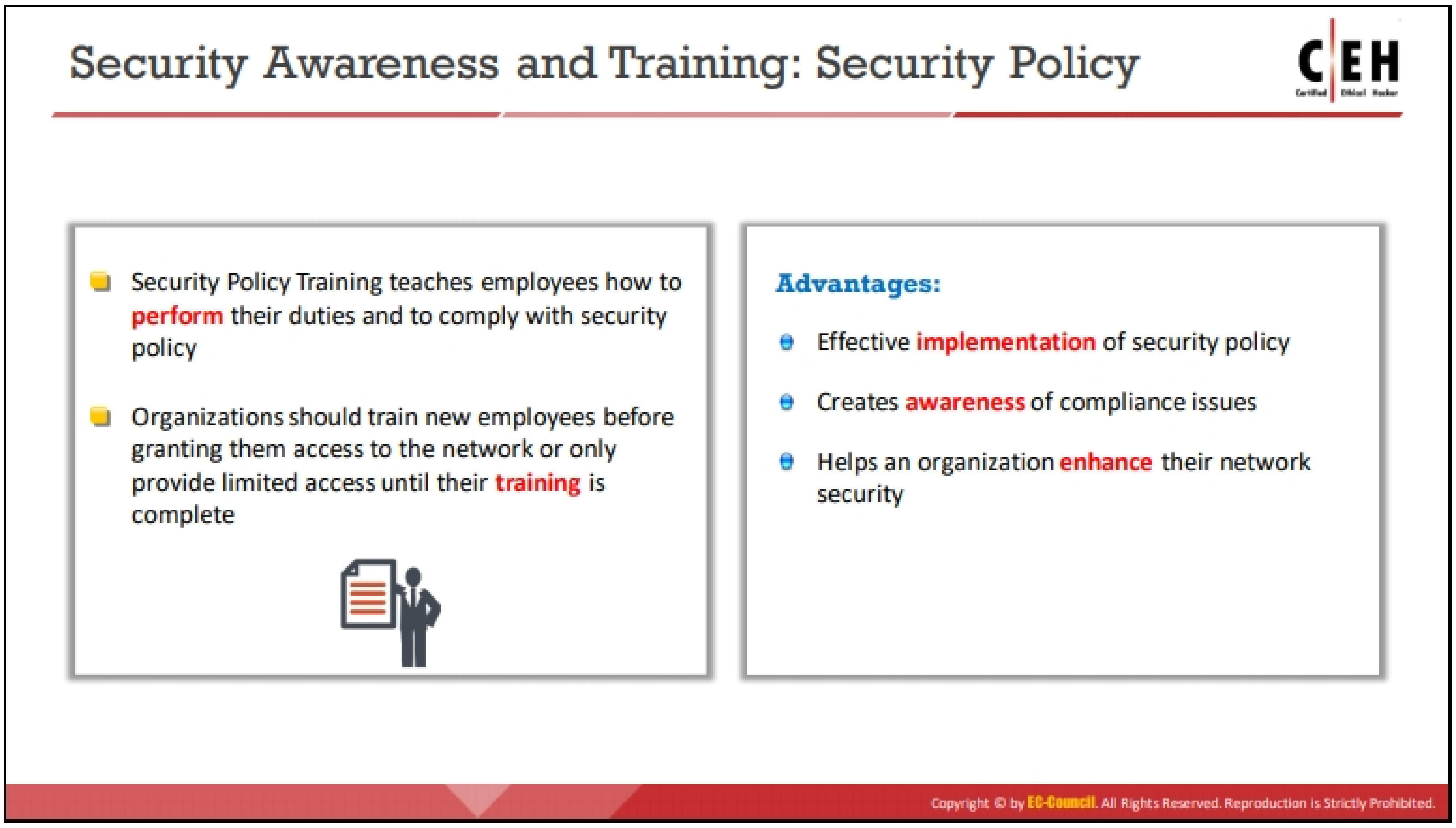
____

____

____

____

____

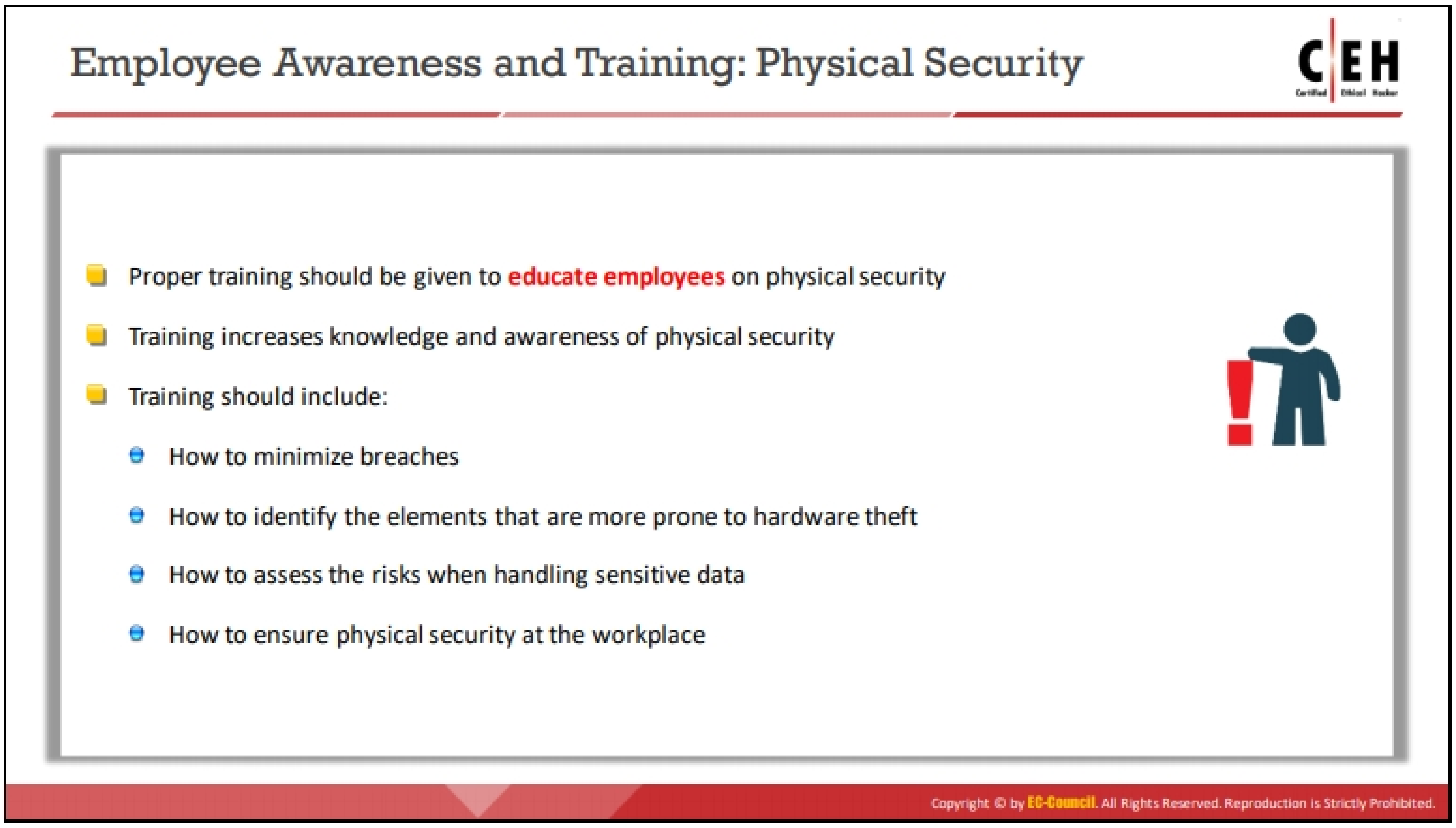


Security Awareness and Training: Security Policy

- Security Policy Training teaches employees how to **perform** their duties and to comply with security policy
- Organizations should train new employees before granting them access to the network or only provide limited access until their **training** is complete

Advantages:

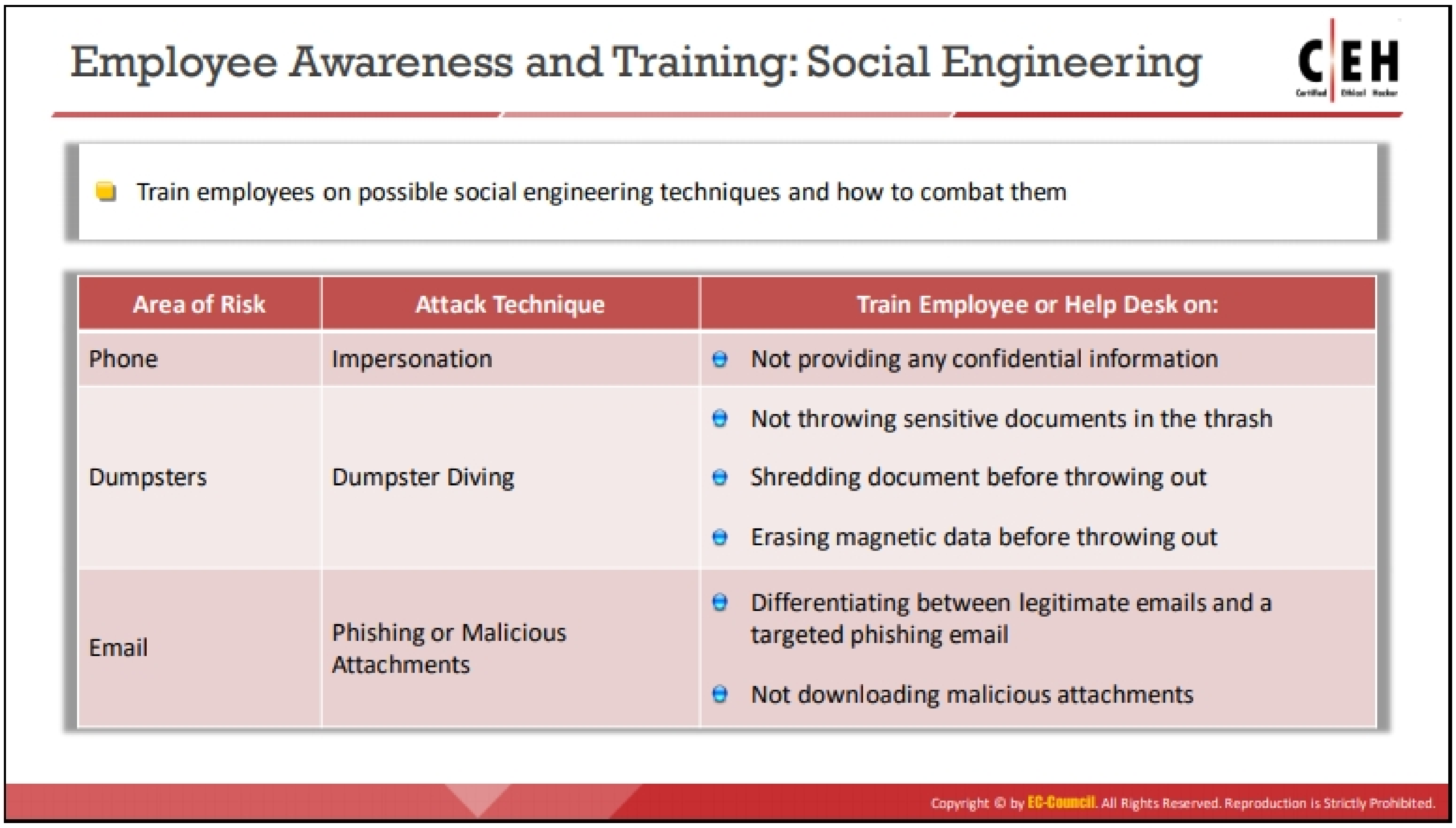
- Effective **implementation** of security policy
- Creates **awareness** of compliance issues
- Helps an organization **enhance** their network security



Employee Awareness and Training: Physical Security

- Proper training should be given to **educate employees** on physical security
- Training increases knowledge and awareness of physical security
- Training should include:
  - How to minimize breaches
  - How to identify the elements that are more prone to hardware theft
  - How to assess the risks when handling sensitive data
  - How to ensure physical security at the workplace

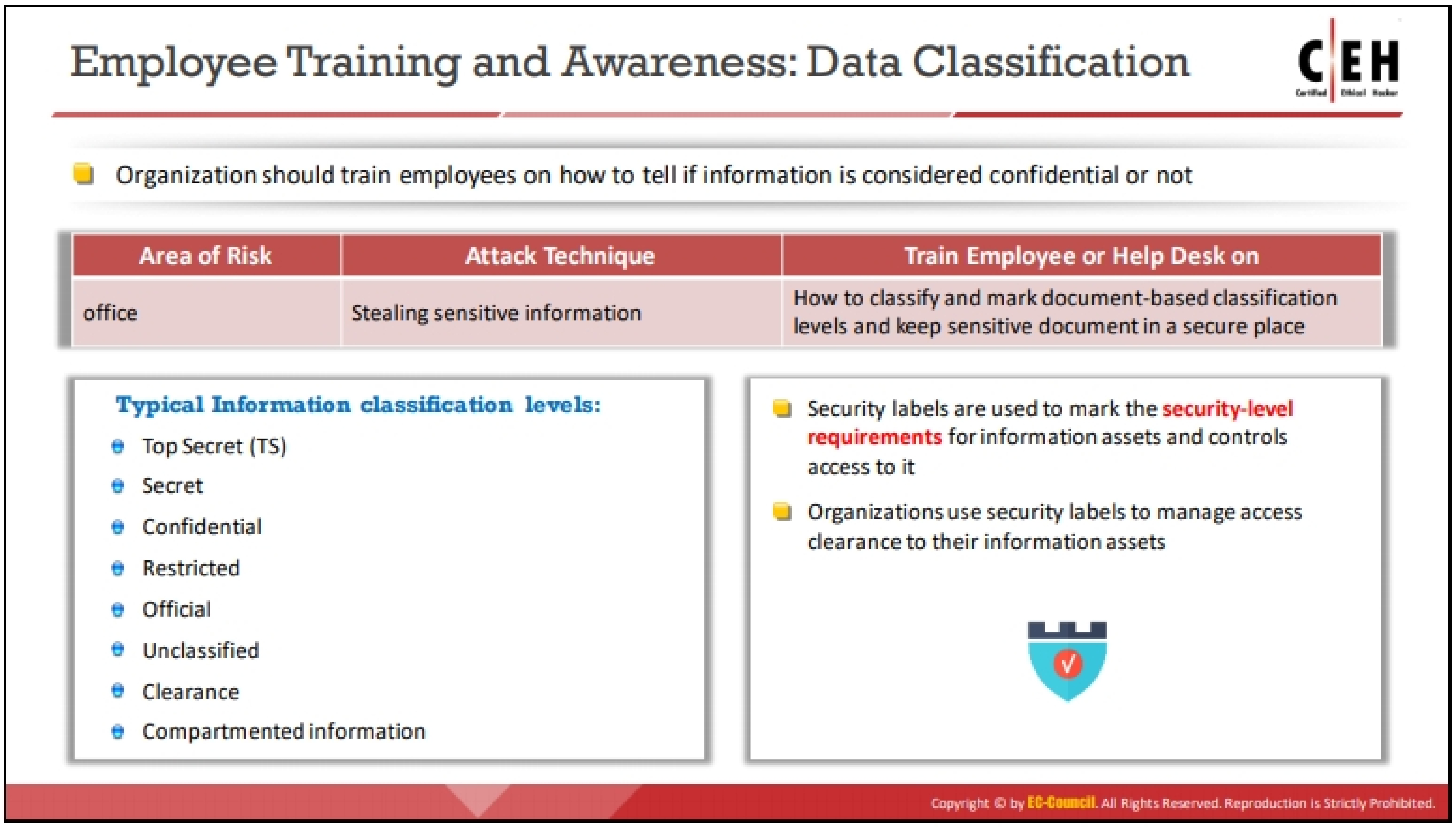
Notes: ______________________________



Employee Awareness and Training: Social Engineering

- Train employees on possible social engineering techniques and how to combat them

Area of Risk	Attack Technique	Train Employee or Help Desk on:
Phone	Impersonation	Not providing any confidential information
Dumpsters	Dumpster Diving	Not throwing sensitive documents in the thrash Shredding document before throwing out Erasing magnetic data before throwing out
Email	Phishing or Malicious Attachments	Differentiating between legitimate emails and a targeted phishing email Not downloading malicious attachments



Employee Training and Awareness: Data Classification

- Organization should train employees on how to tell if information is considered confidential or not

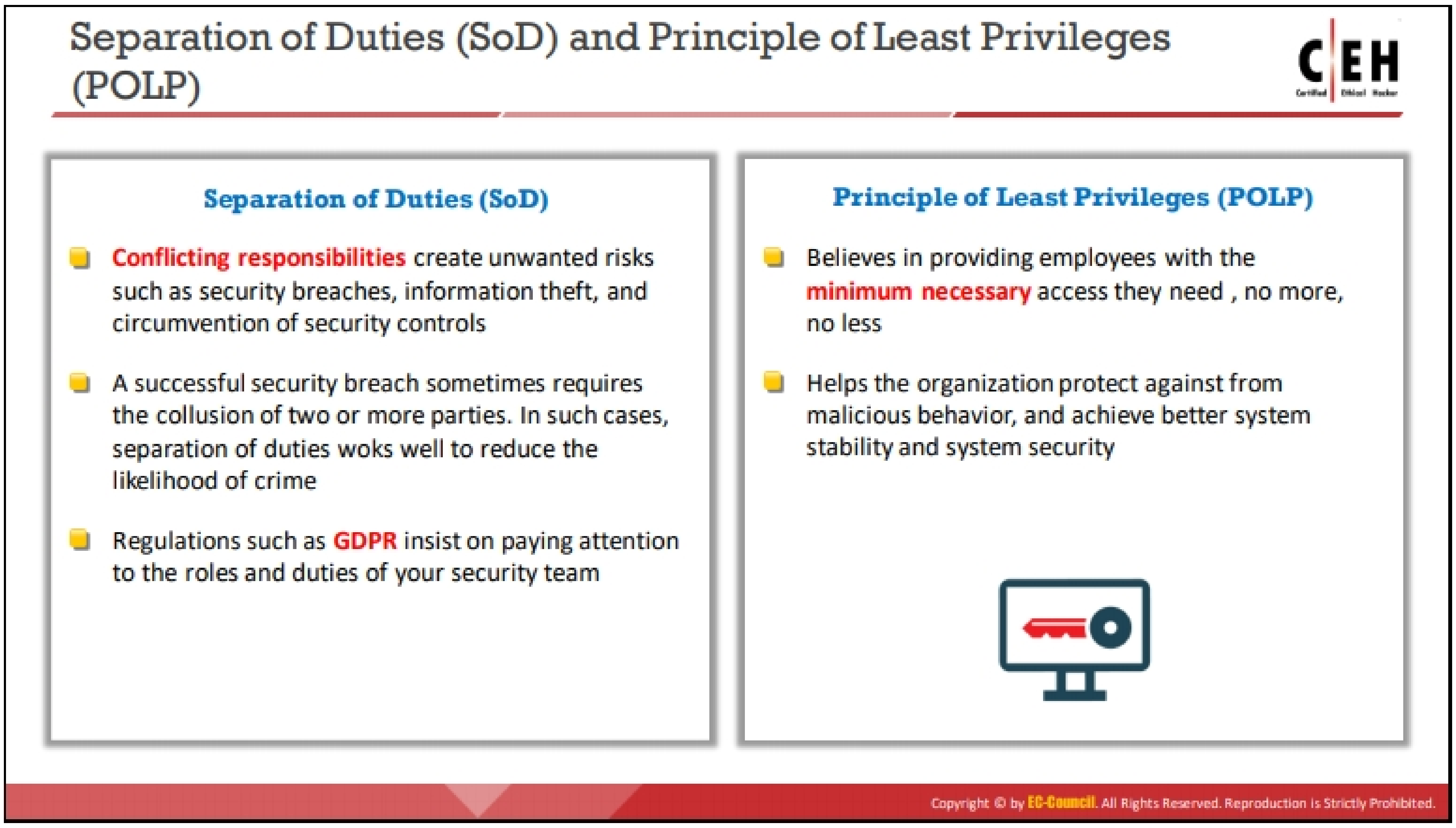
Area of Risk	Attack Technique	Train Employee or Help Desk on
office	Stealing sensitive information	How to classify and mark document-based classification levels and keep sensitive document in a secure place

Typical Information classification levels:

- Top Secret (TS)
- Secret
- Confidential
- Restricted
- Official
- Unclassified
- Clearance
- Compartmented information

- Security labels are used to mark the **security-level requirements** for information assets and controls access to it
- Organizations use security labels to manage access clearance to their information assets

Notes: ____



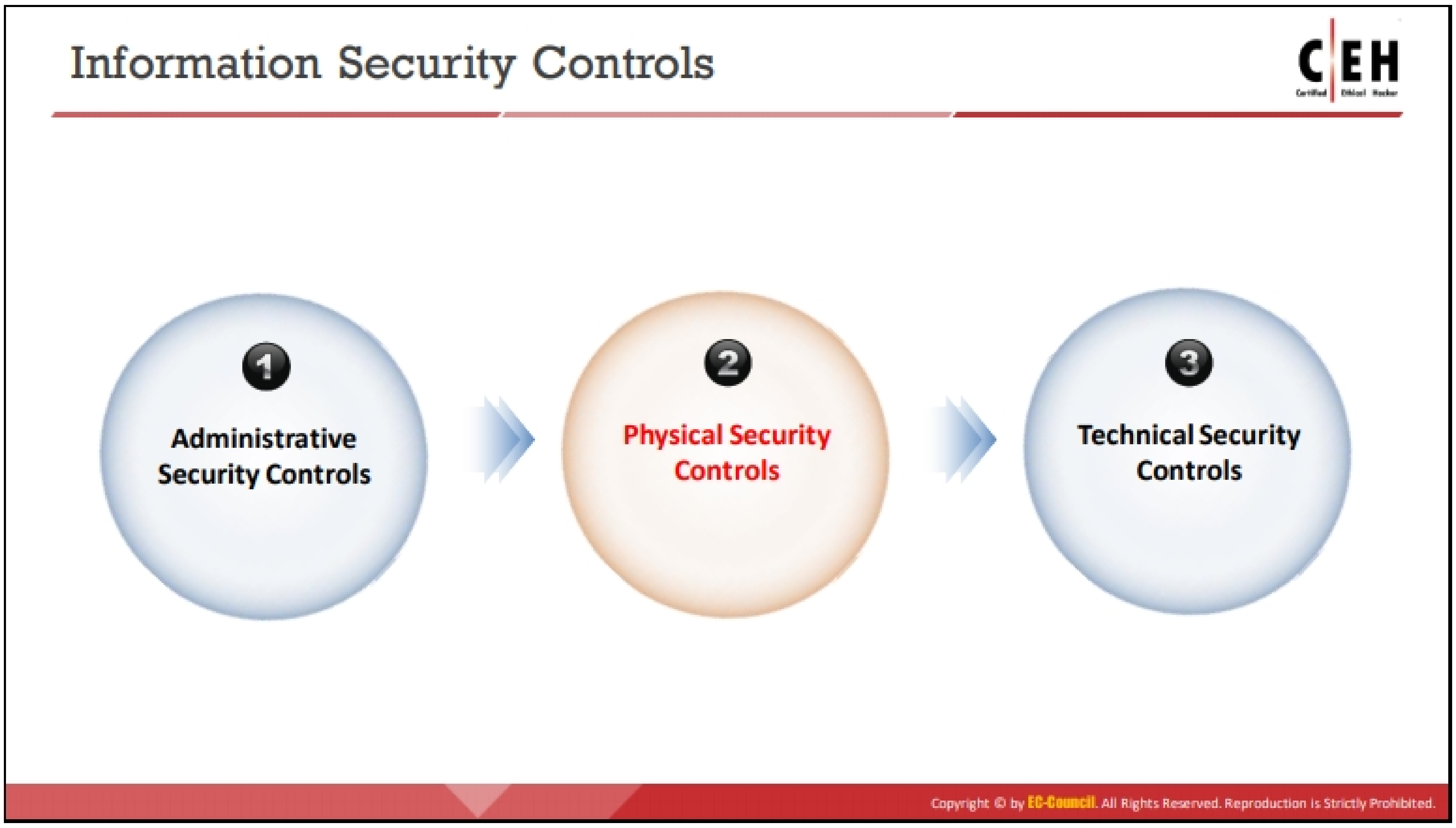
Separation of Duties (SoD) and Principle of Least Privileges (POLP)

Separation of Duties (SoD)

- **Conflicting responsibilities** create unwanted risks such as security breaches, information theft, and circumvention of security controls
- A successful security breach sometimes requires the collusion of two or more parties. In such cases, separation of duties woks well to reduce the likelihood of crime
- Regulations such as **GDPR** insist on paying attention to the roles and duties of your security team

Principle of Least Privileges (POLP)

- Believes in providing employees with the **minimum necessary** access they need , no more, no less
- Helps the organization protect against from malicious behavior, and achieve better system stability and system security



Information Security Controls

1
Administrative Security Controls
2
Physical Security Controls
3
Technical Security Controls

Notes: ____

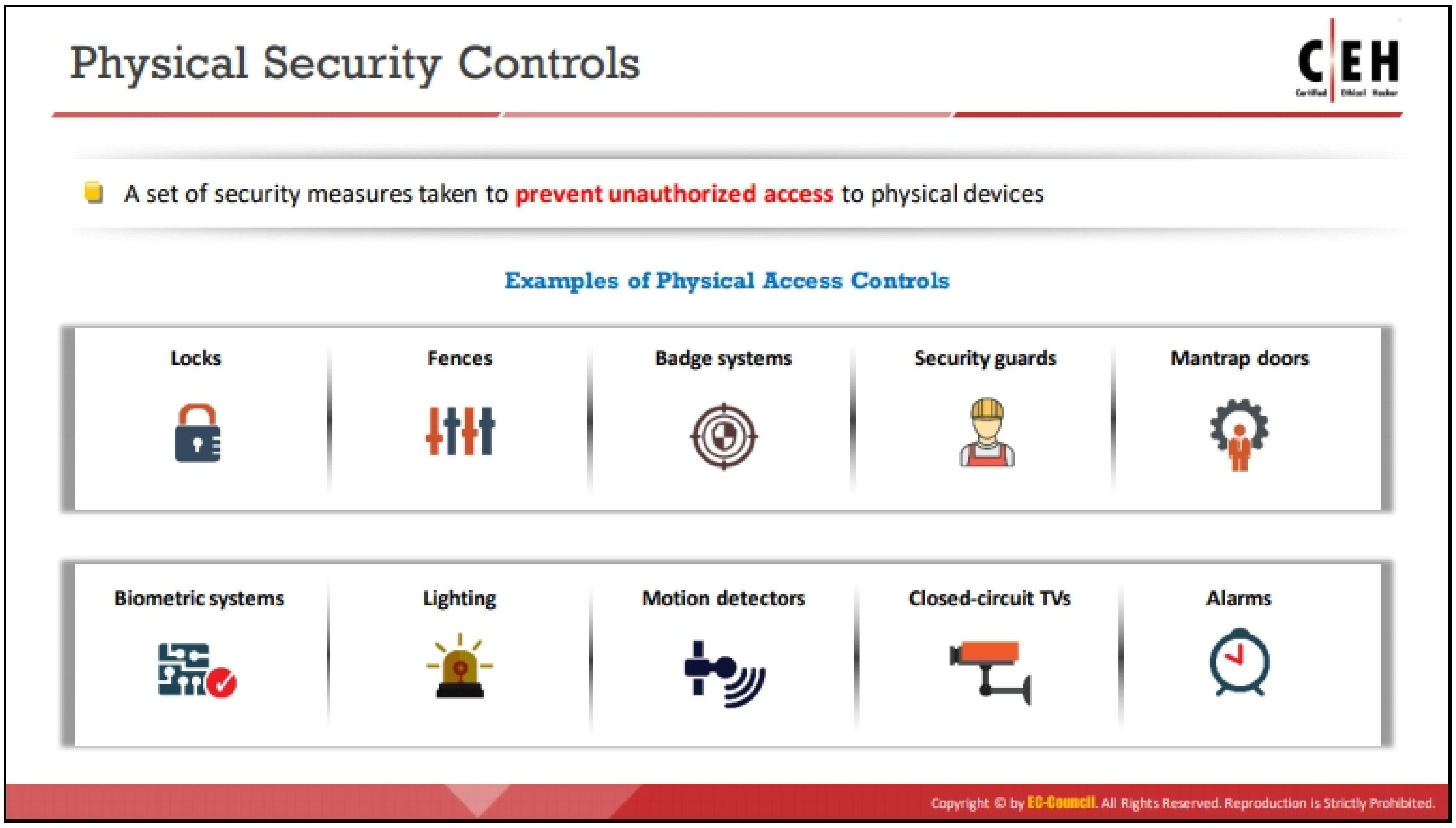
____

____

____

____

____

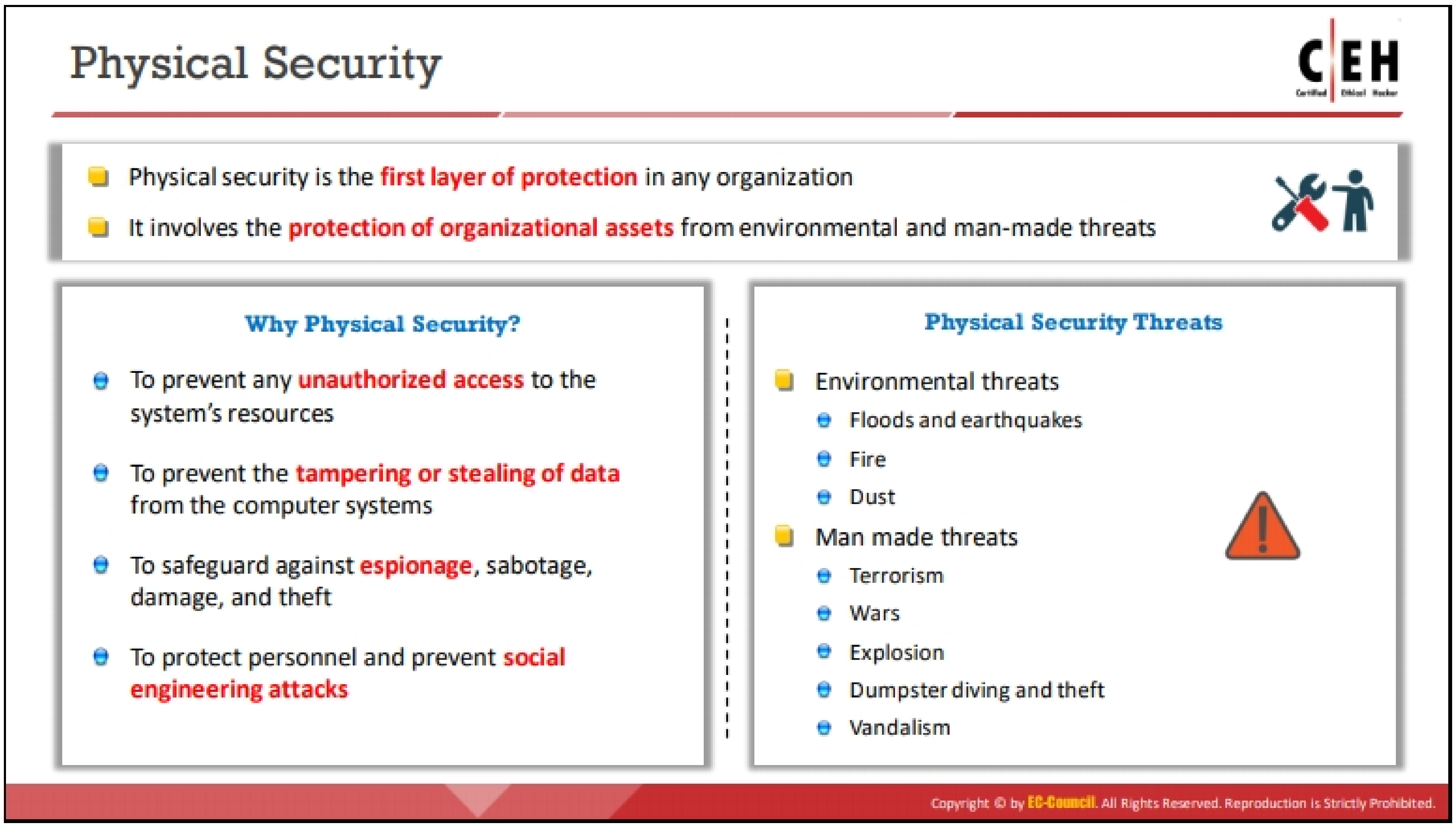


Physical Security Controls

- A set of security measures taken to **prevent unauthorized access** to physical devices

Examples of Physical Access Controls

- Locks
- Fences
- Badge systems
- Security guards
- Mantrap doors
- Biometric systems
- Lighting
- Motion detectors
- Closed-circuit TVs
- Alarms



Physical Security

- Physical security is the **first layer of protection** in any organization
- It involves the **protection of organizational assets** from environmental and man-made threats

Why Physical Security?

- To prevent any **unauthorized access** to the system's resources
- To prevent the **tampering or stealing of data** from the computer systems
- To safeguard against **espionage**, sabotage, damage, and theft
- To protect personnel and prevent **social engineering attacks**

Physical Security Threats

- Environmental threats
  - Floods and earthquakes
  - Fire
  - Dust
- Man made threats
  - Terrorism
  - Wars
  - Explosion
  - Dumpster diving and theft
  - Vandalism

Notes: ____

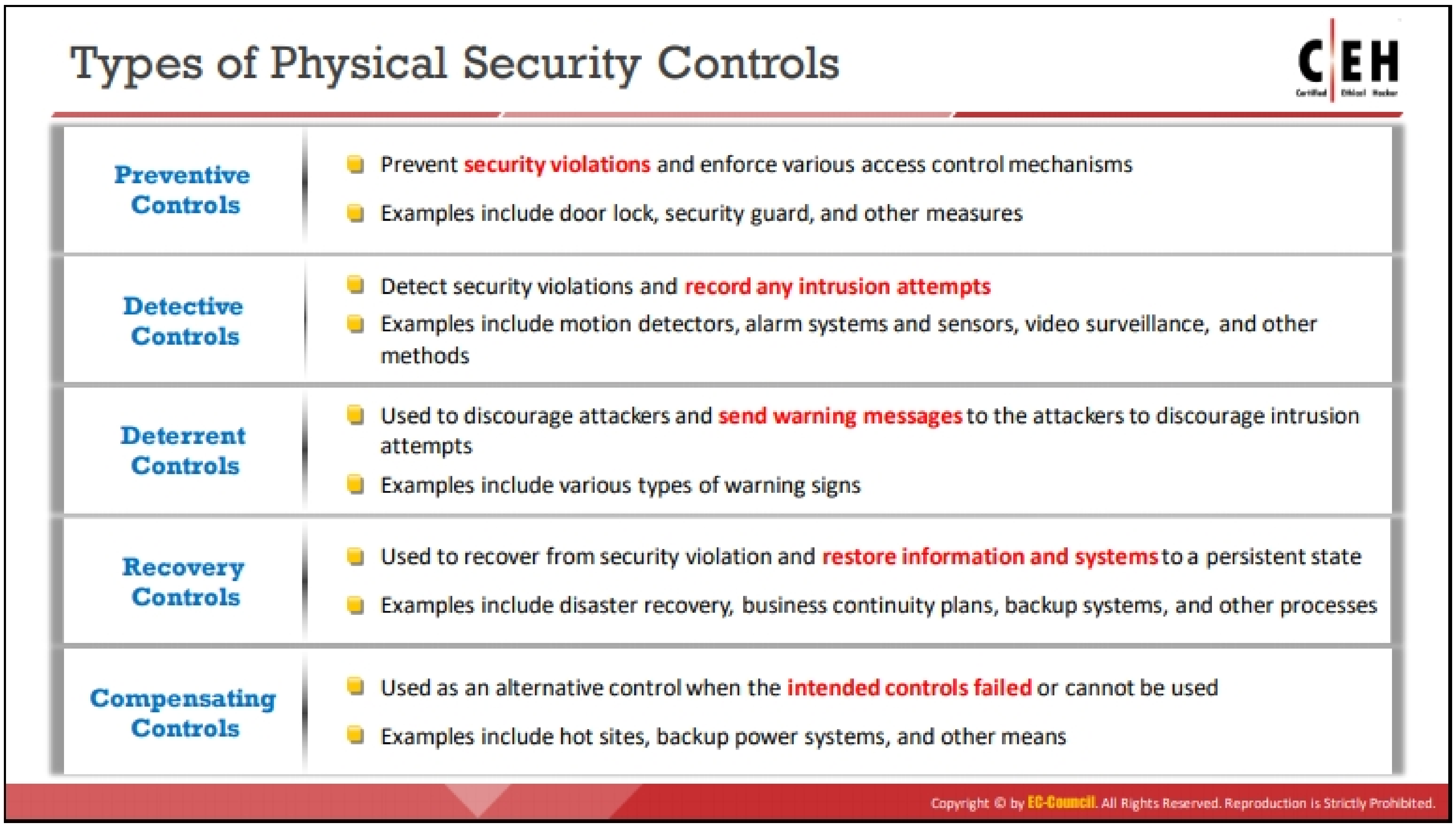
____

____

____

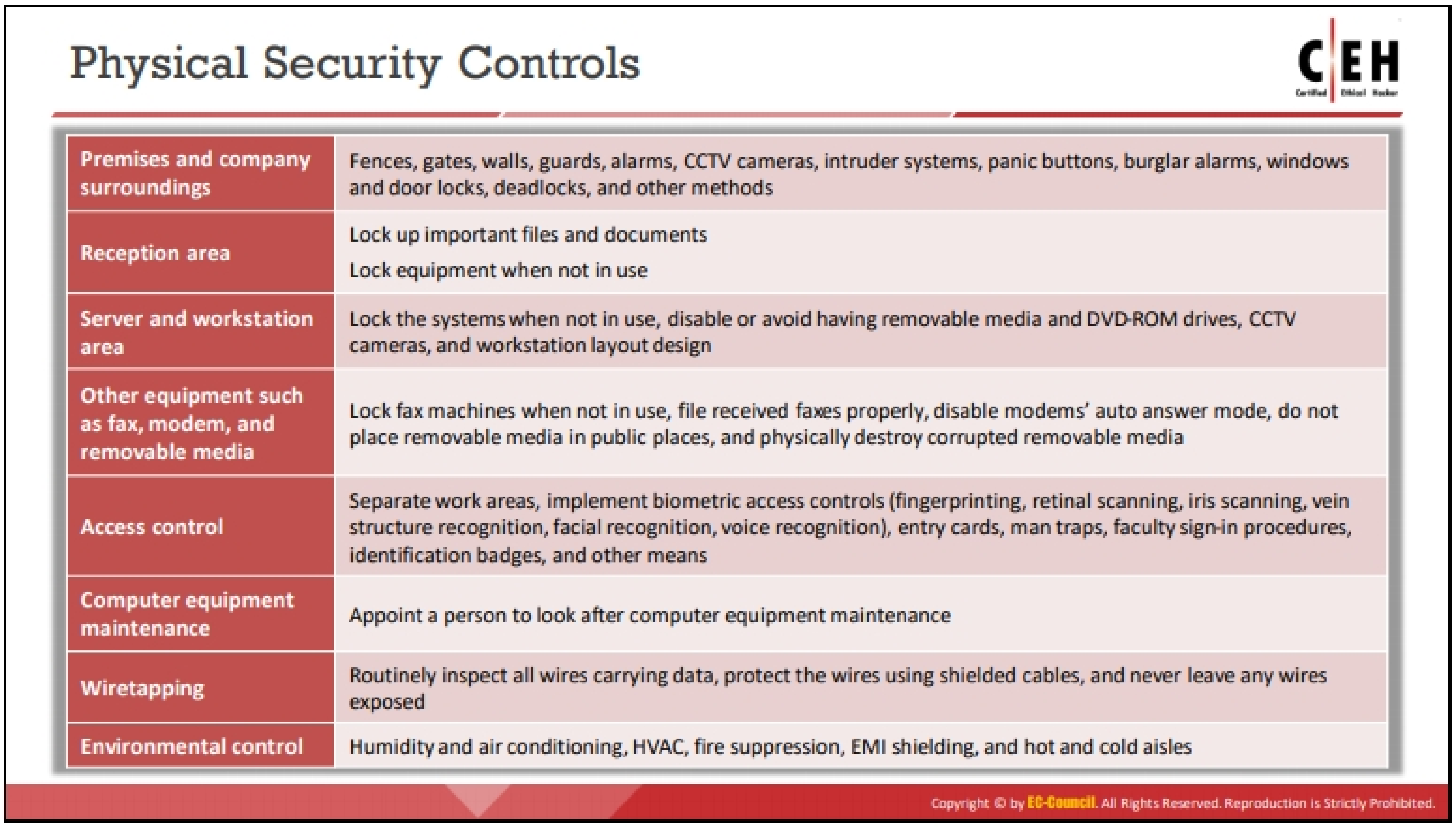
____

____



Types of Physical Security Controls

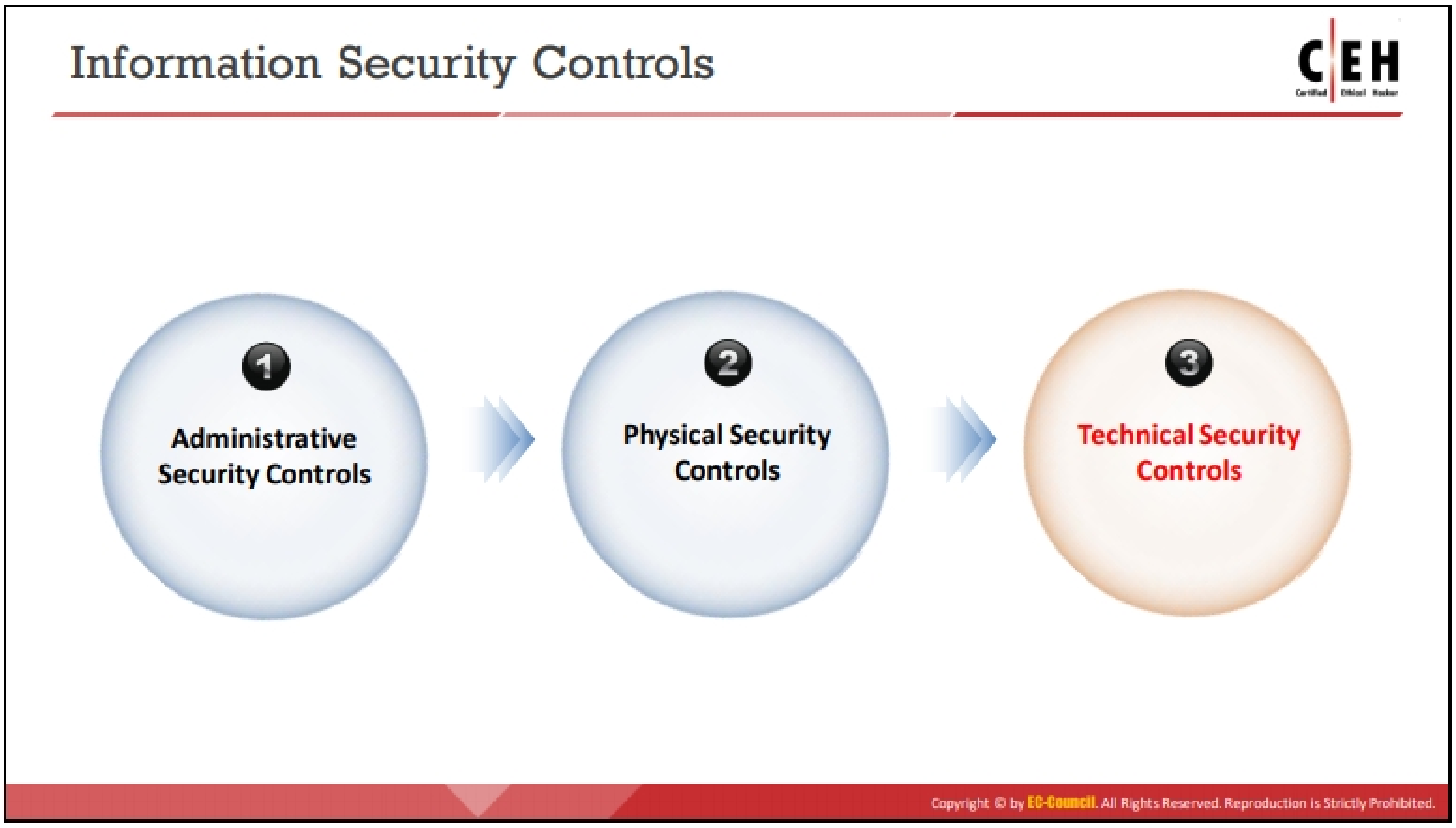
Preventive Controls	- Prevent **security violations** and enforce various access control mechanisms - Examples include door lock, security guard, and other measures
Detective Controls	- Detect security violations and **record any intrusion attempts** - Examples include motion detectors, alarm systems and sensors, video surveillance, and other methods
Deterrent Controls	- Used to discourage attackers and **send warning messages** to the attackers to discourage intrusion attempts - Examples include various types of warning signs
Recovery Controls	- Used to recover from security violation and **restore information and systems** to a persistent state - Examples include disaster recovery, business continuity plans, backup systems, and other processes
Compensating Controls	- Used as an alternative control when the **intended controls failed** or cannot be used - Examples include hot sites, backup power systems, and other means



Physical Security Controls

Premises and company surroundings	Fences, gates, walls, guards, alarms, CCTV cameras, intruder systems, panic buttons, burglar alarms, windows and door locks, deadlocks, and other methods
Reception area	Lock up important files and documents Lock equipment when not in use
Server and workstation area	Lock the systems when not in use, disable or avoid having removable media and DVD-ROM drives, CCTV cameras, and workstation layout design
Other equipment such as fax, modem, and removable media	Lock fax machines when not in use, file received faxes properly, disable modems' auto answer mode, do not place removable media in public places, and physically destroy corrupted removable media
Access control	Separate work areas, implement biometric access controls (fingerprinting, retinal scanning, iris scanning, vein structure recognition, facial recognition, voice recognition), entry cards, man traps, faculty sign-in procedures, identification badges, and other means
Computer equipment maintenance	Appoint a person to look after computer equipment maintenance
Wiretapping	Routinely inspect all wires carrying data, protect the wires using shielded cables, and never leave any wires exposed
Environmental control	Humidity and air conditioning, HVAC, fire suppression, EMI shielding, and hot and cold aisles

Notes: ______________________________

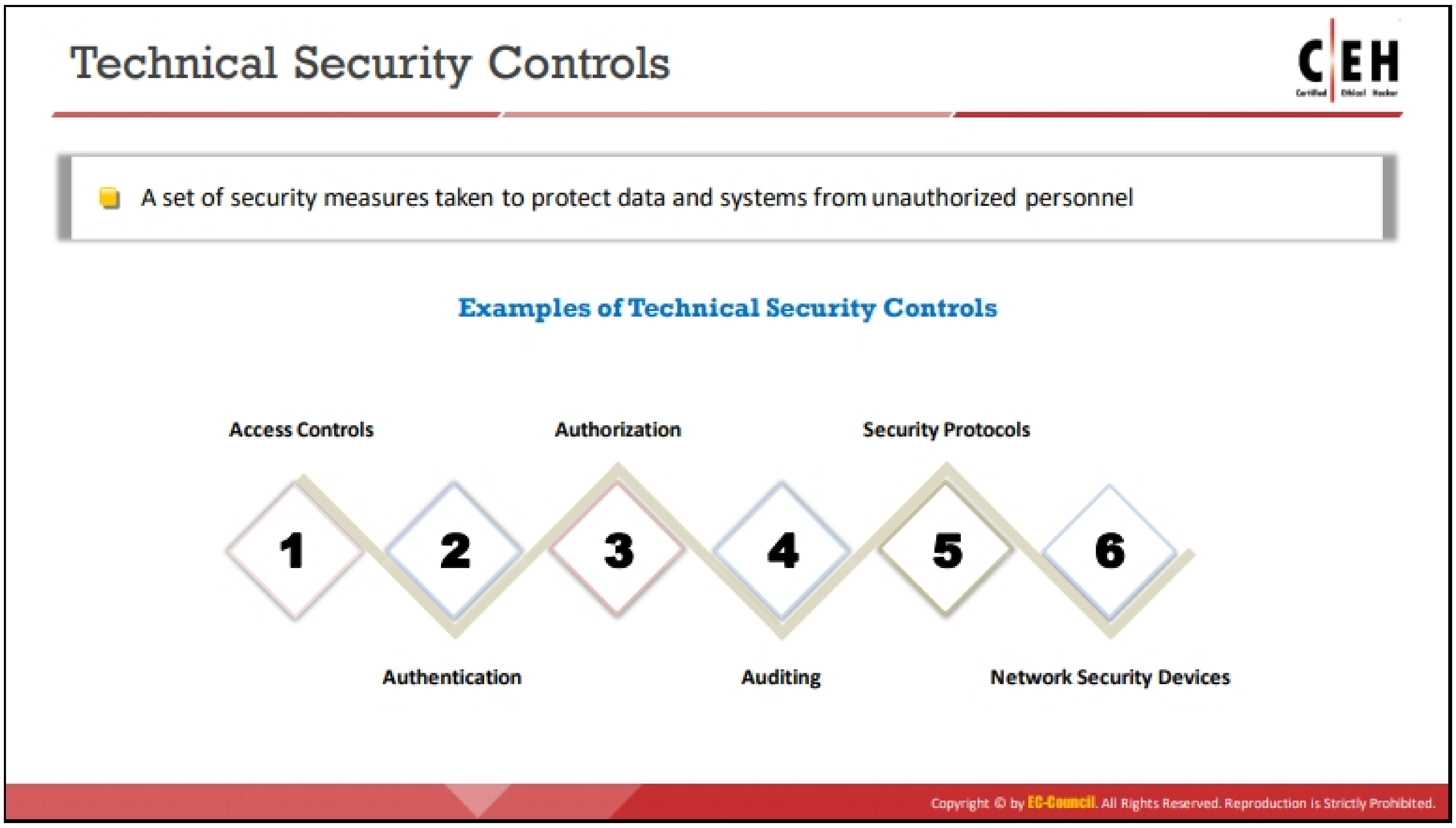


Information Security Controls

1 Administrative Security Controls

2 Physical Security Controls

3 Technical Security Controls



Technical Security Controls

- A set of security measures taken to protect data and systems from unauthorized personnel

Examples of Technical Security Controls

1 Access Controls

2 Authentication

3 Authorization

4 Auditing

5 Security Protocols

6 Network Security Devices

Notes: ____

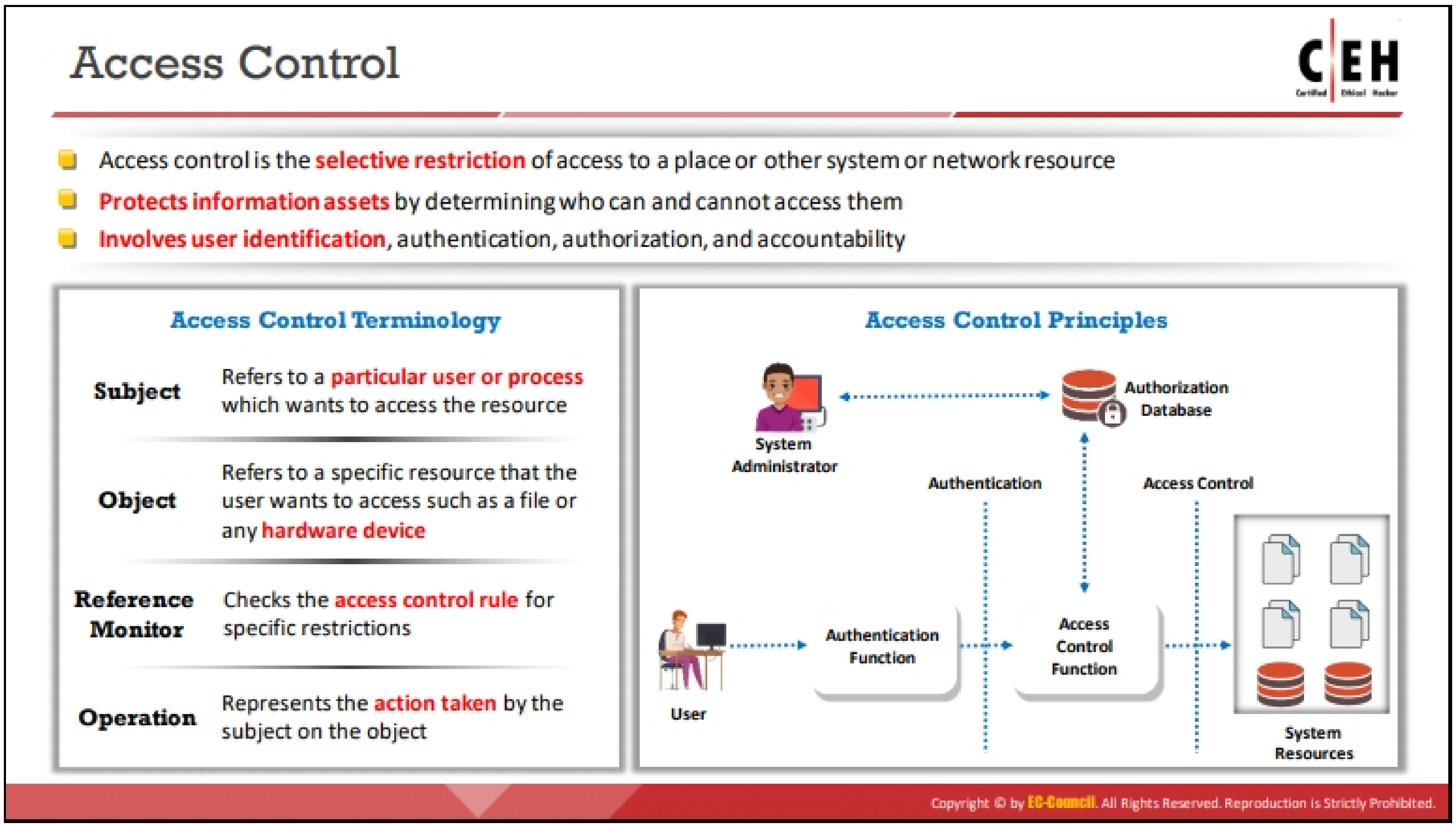
____

____

____

____

____



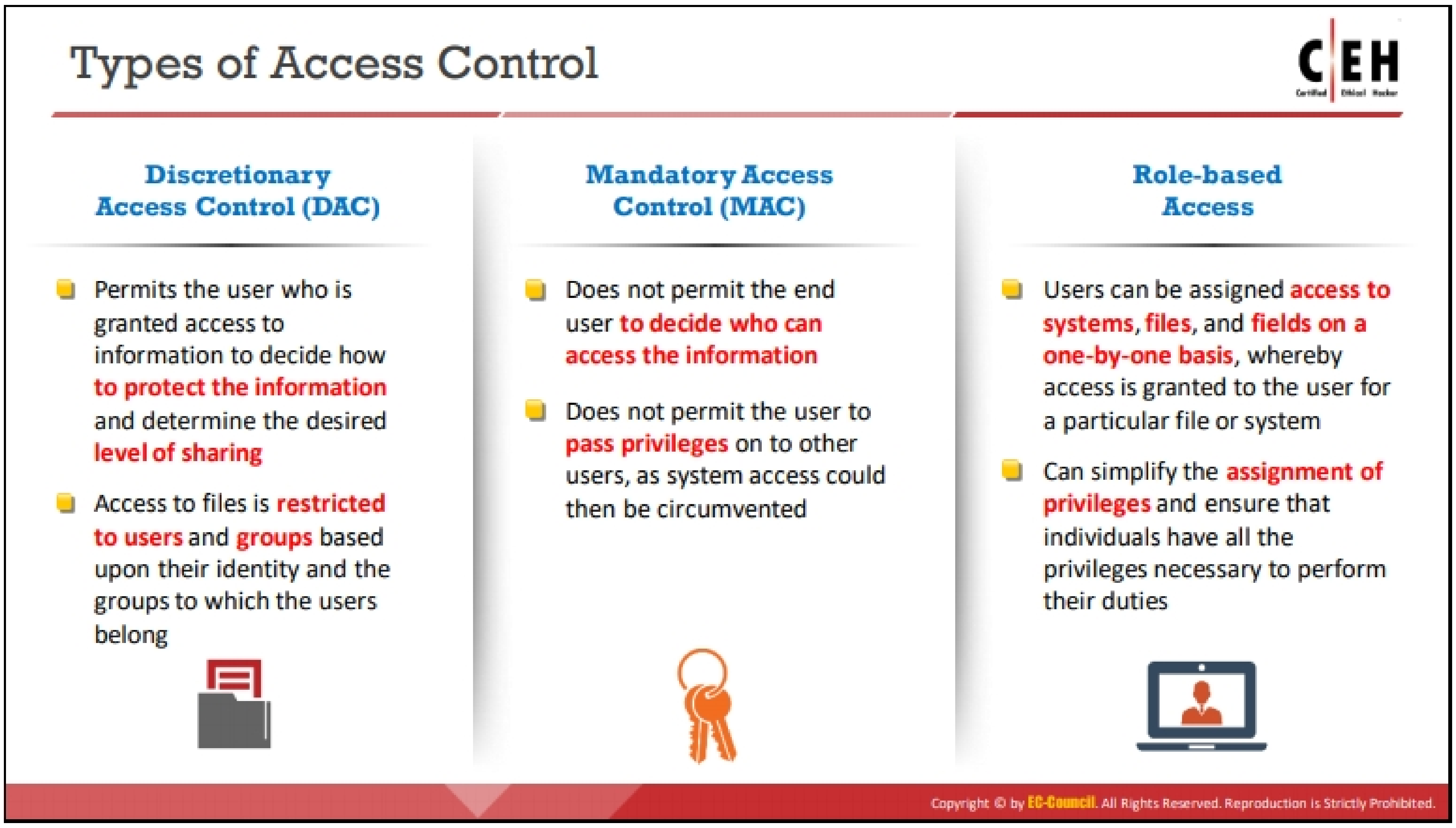
Access Control

- Access control is the **selective restriction** of access to a place or other system or network resource
- **Protects information assets** by determining who can and cannot access them
- **Involves user identification**, authentication, authorization, and accountability

Access Control Terminology

Subject	Refers to a **particular user or process** which wants to access the resource
Object	Refers to a specific resource that the user wants to access such as a file or any **hardware device**
Reference Monitor	Checks the **access control rule** for specific restrictions
Operation	Represents the **action taken** by the subject on the object

Access Control Principles



Types of Access Control

Discretionary Access Control (DAC)

- Permits the user who is granted access to information to decide how **to protect the information** and determine the desired **level of sharing**
- Access to files is **restricted to users** and **groups** based upon their identity and the groups to which the users belong

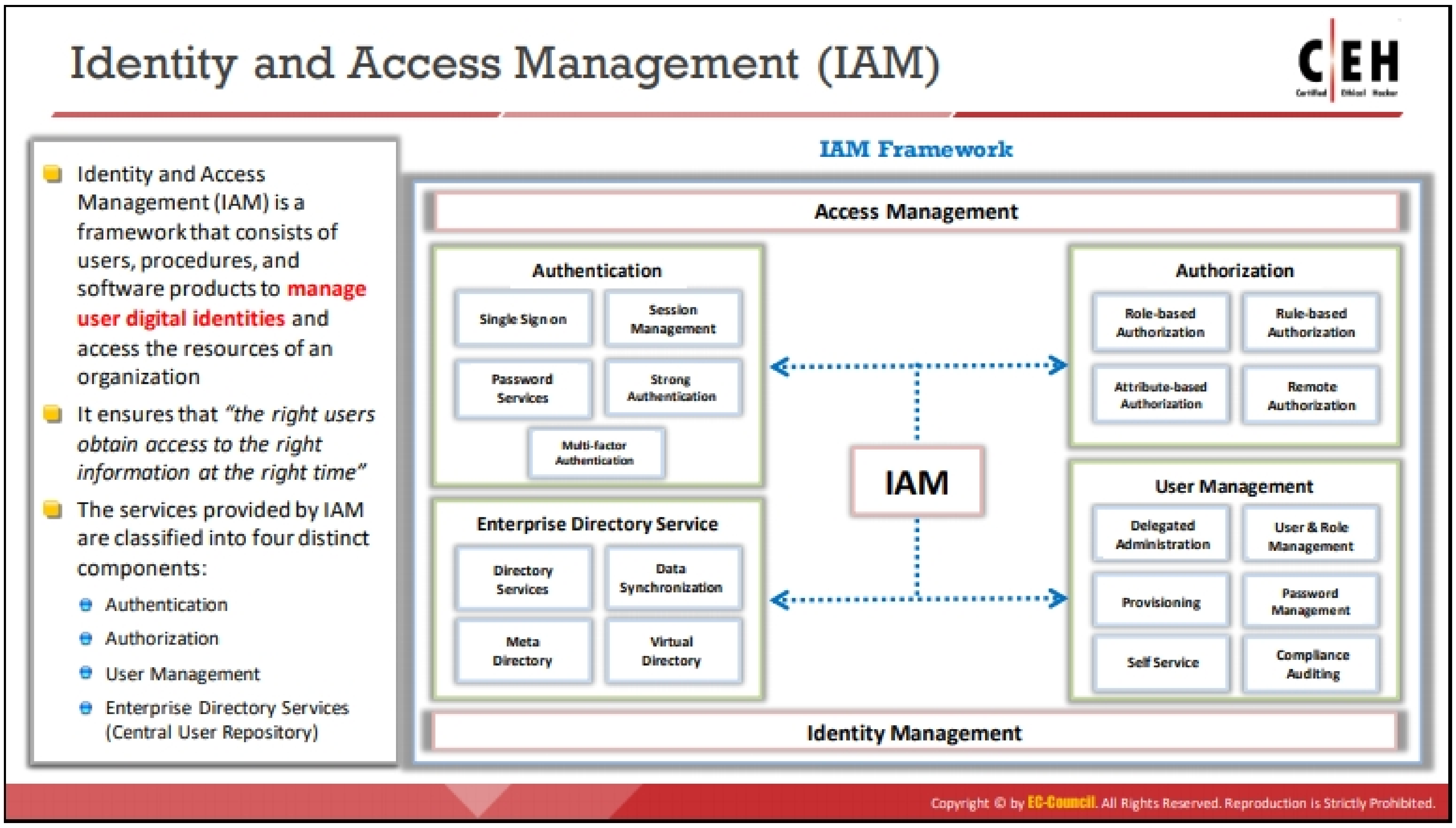
Mandatory Access Control (MAC)

- Does not permit the end user **to decide who can access the information**
- Does not permit the user to **pass privileges** on to other users, as system access could then be circumvented

Role-based Access

- Users can be assigned **access to systems**, **files**, and **fields on a one-by-one basis**, whereby access is granted to the user for a particular file or system
- Can simplify the **assignment of privileges** and ensure that individuals have all the privileges necessary to perform their duties

Notes:



Identity and Access Management (IAM)

- Identity and Access Management (IAM) is a framework that consists of users, procedures, and software products to **manage user digital identities** and access the resources of an organization
- It ensures that *"the right users obtain access to the right information at the right time"*
- The services provided by IAM are classified into four distinct components:
  - Authentication
  - Authorization
  - User Management
  - Enterprise Directory Services (Central User Repository)

IAM Framework

Access Management

Authentication
Single Sign on
Session Management
Password Services
Strong Authentication
Multi-factor Authentication

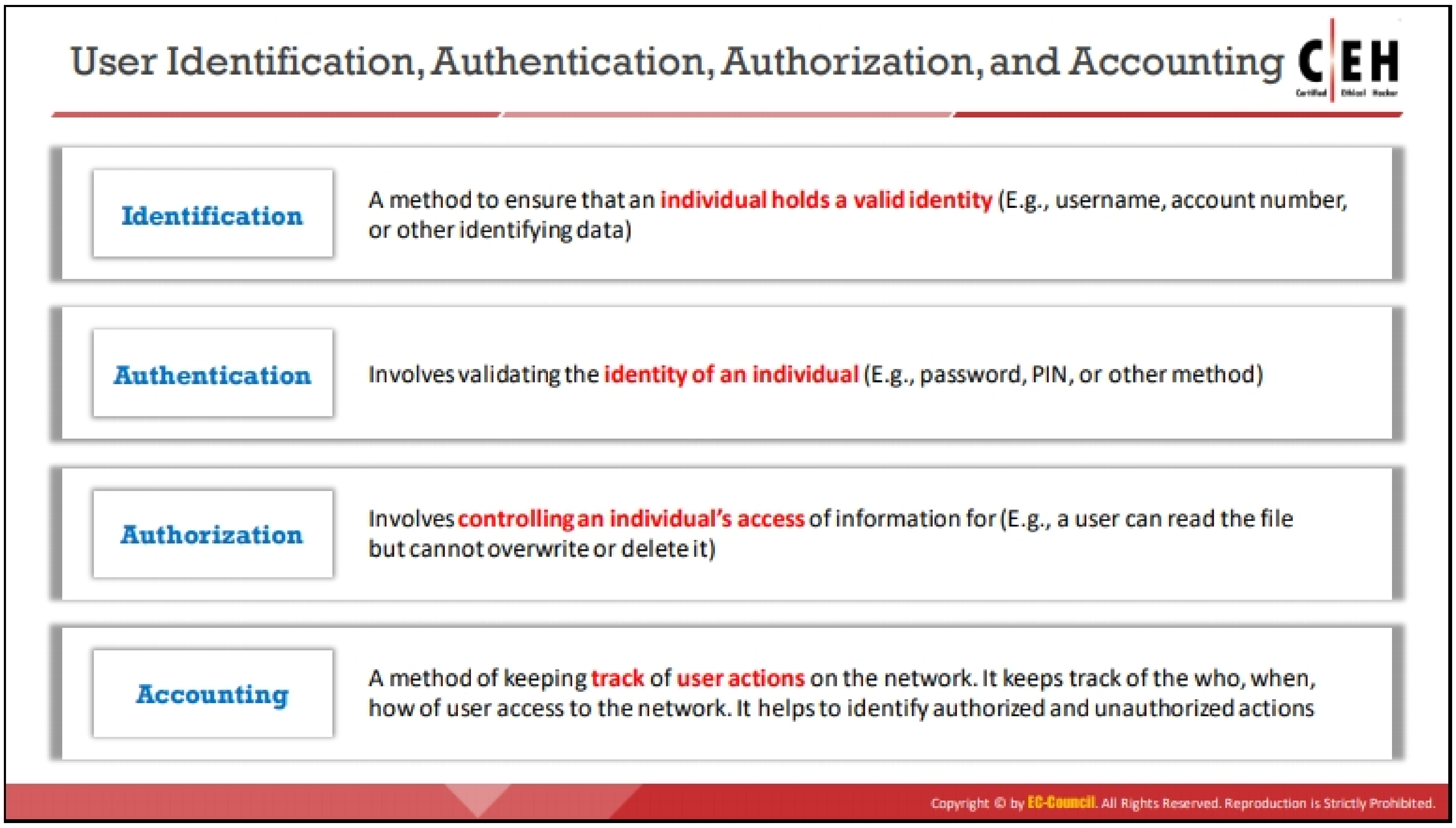
Authorization
Role-based Authorization
Rule-based Authorization
Attribute-based Authorization
Remote Authorization

IAM

Enterprise Directory Service
Directory Services
Data Synchronization
Meta Directory
Virtual Directory

User Management
Delegated Administration
User & Role Management
Provisioning
Password Management
Self Service
Compliance Auditing

Identity Management



User Identification, Authentication, Authorization, and Accounting

Identification	A method to ensure that an **individual holds a valid identity** (E.g., username, account number, or other identifying data)
Authentication	Involves validating the **identity of an individual** (E.g., password, PIN, or other method)
Authorization	Involves **controlling an individual's access** of information for (E.g., a user can read the file but cannot overwrite or delete it)
Accounting	A method of keeping **track** of **user actions** on the network. It keeps track of the who, when, how of user access to the network. It helps to identify authorized and unauthorized actions

Notes: ____

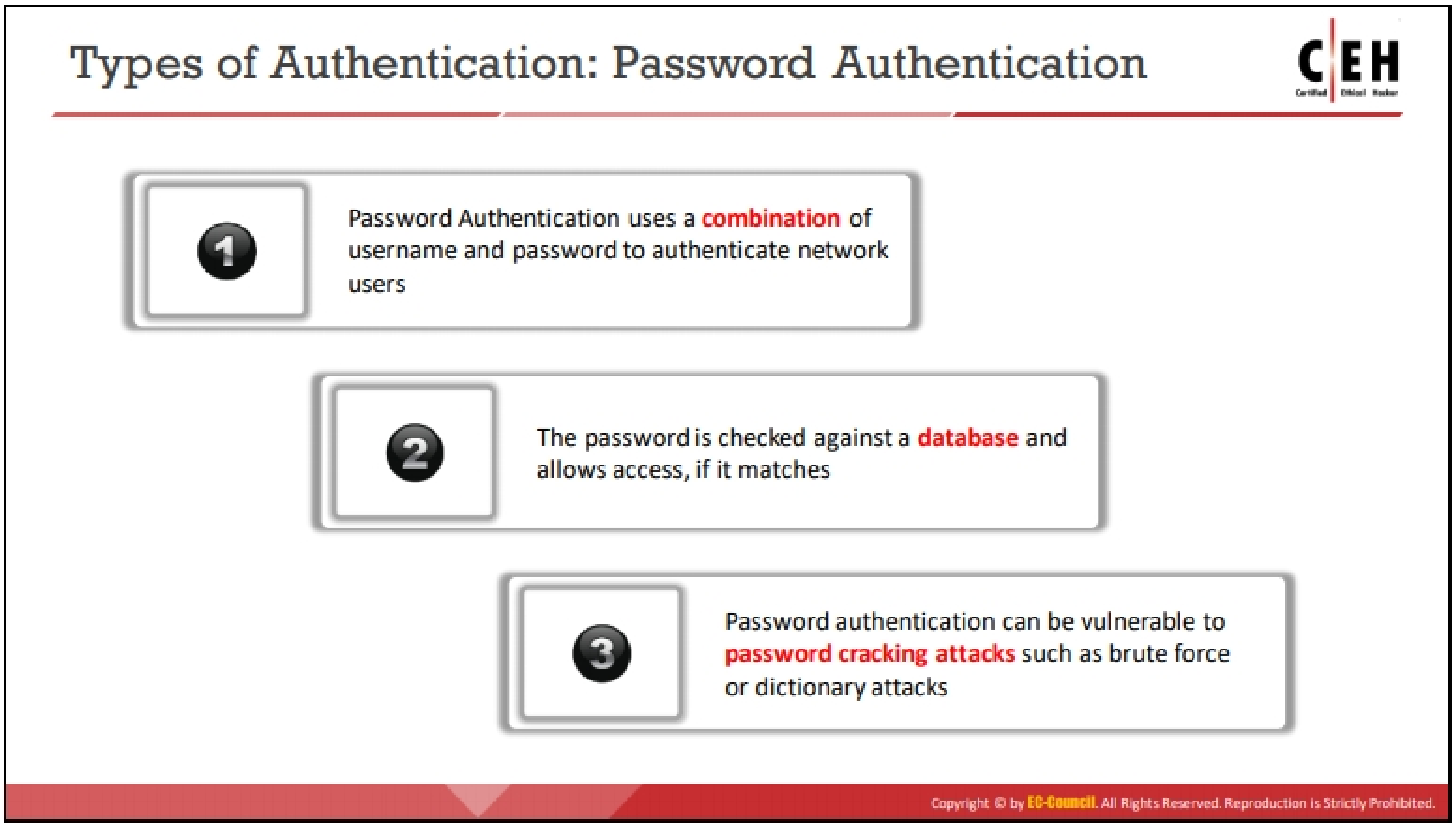
____

____

____

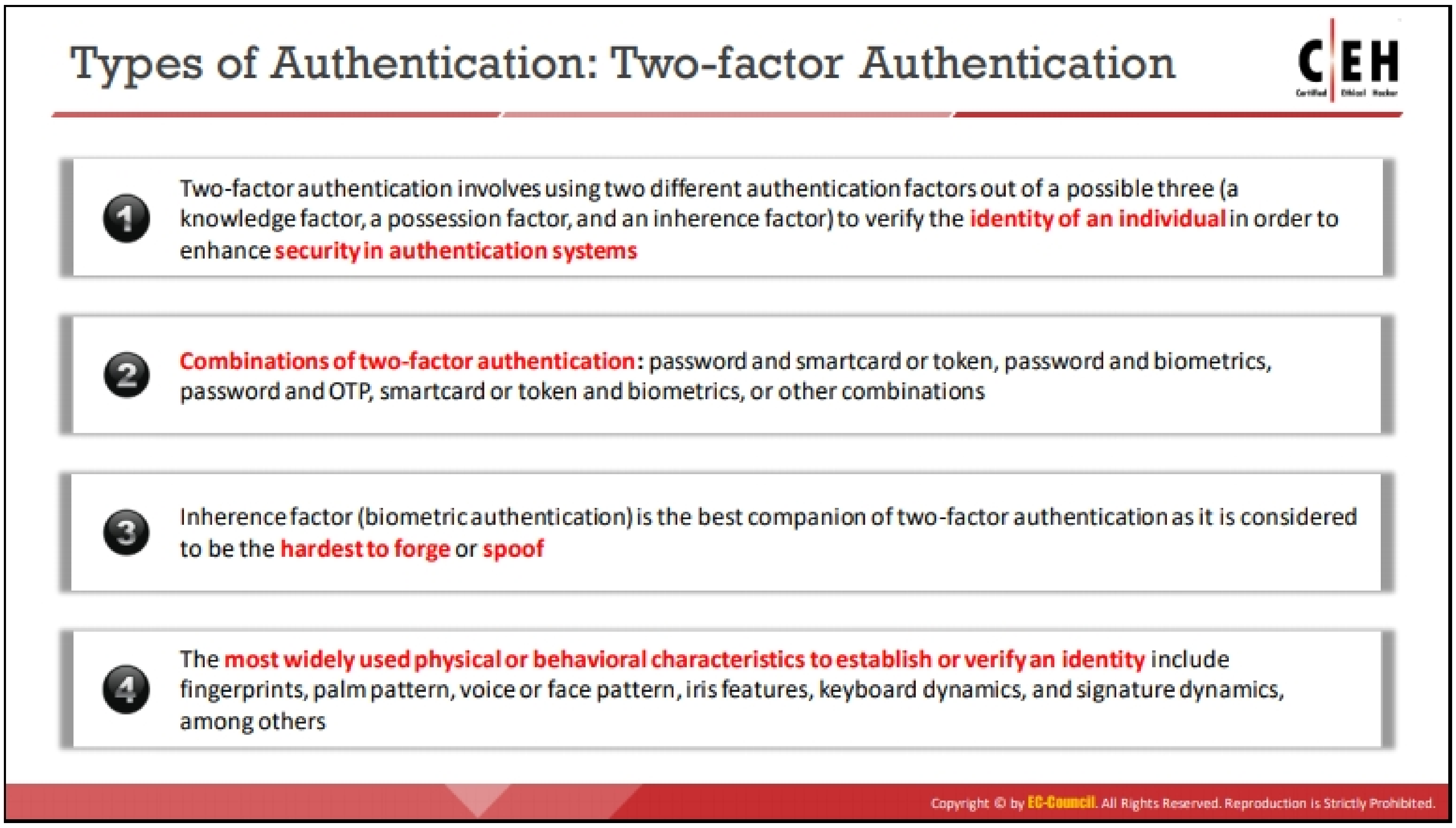
____

____



Types of Authentication: Password Authentication

1. Password Authentication uses a **combination** of username and password to authenticate network users
2. The password is checked against a **database** and allows access, if it matches
3. Password authentication can be vulnerable to **password cracking attacks** such as brute force or dictionary attacks



Types of Authentication: Two-factor Authentication

1. Two-factor authentication involves using two different authentication factors out of a possible three (a knowledge factor, a possession factor, and an inherence factor) to verify the **identity of an individual** in order to enhance **security in authentication systems**
2. **Combinations of two-factor authentication**: password and smartcard or token, password and biometrics, password and OTP, smartcard or token and biometrics, or other combinations
3. Inherence factor (biometric authentication) is the best companion of two-factor authentication as it is considered to be the **hardest to forge** or **spoof**
4. The **most widely used physical or behavioral characteristics to establish or verify an identity** include fingerprints, palm pattern, voice or face pattern, iris features, keyboard dynamics, and signature dynamics, among others

Notes:

Types of Authentication: Biometrics

- Biometrics refers to the **identification of individuals** based on their physical characteristics

Biometric Identification Techniques

Fingerprinting

- **Ridges** and **furrows** on the surface of the fingertip, which are individually **unique**

Retinal Scanning

- **Analyzes** the layer of blood vessels at the back of their eyes

Iris Scanning

- Analyzes the colored part of the eye

Vein Structure Recognition

- **Analyzes** the thickness and location of veins

Face Recognition

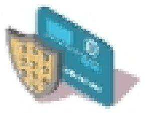
- Analyzes the pattern of **facial features**

Voice Recognition

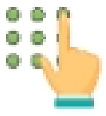
- Analyzes an **individual's vocal pattern**

Types of Authentication: Smart Card Authentication

- A smartcard is a small **computer chip device** that holds the personal information required to authenticate the user



- Users must insert their Smartcards into readers and their **Personal Identification Number** (PIN) to complete authentication



- Smartcard Authentication is a **cryptography-based authentication** method that provides stronger security than password authentication

Notes: ____

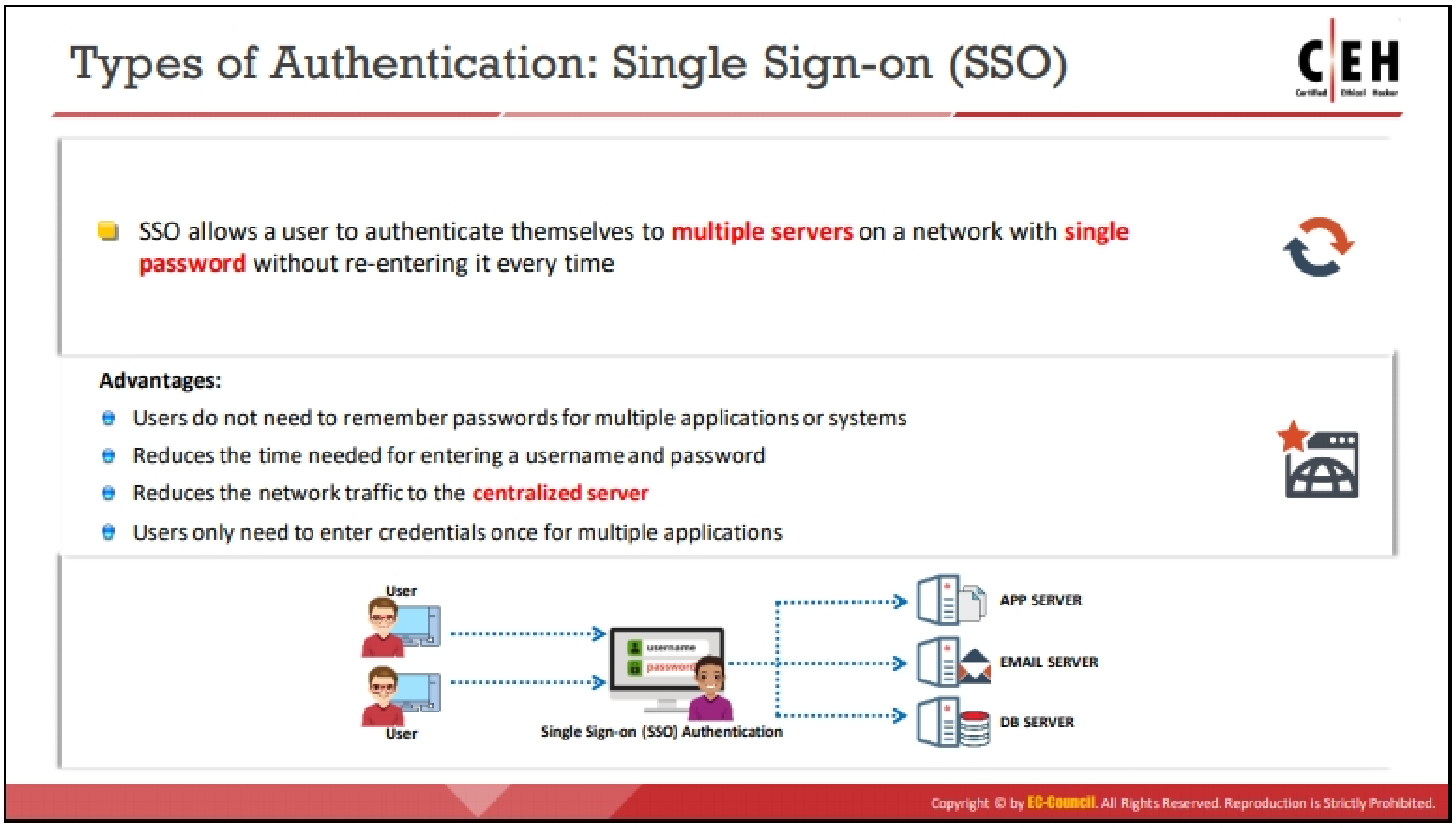
____

____

____

____

____



Types of Authentication: Single Sign-on (SSO)

- SSO allows a user to authenticate themselves to **multiple servers** on a network with **single password** without re-entering it every time

Advantages:

- Users do not need to remember passwords for multiple applications or systems
- Reduces the time needed for entering a username and password
- Reduces the network traffic to the **centralized server**
- Users only need to enter credentials once for multiple applications

Types of Authorization

- Authorization involves **controlling an individual's access** of information (E.g., the user can read the file but not overwrite or delete it)

Types of Authorization Systems

Centralized Authorization

- Authorization for network access is done through a **single centralized** authorization unit
- Maintains a **single database** for authorizing all the network resources or applications
- **An easy and inexpensive** authorization approach

Implicit Authorization

- Users can access the requested resource **on behalf** of others
- The access request goes through a **primary resource** to access the requested resource

Decentralized Authorization

- Each network resource maintains its **authorization unit** and locally performs authorization
- Maintains its **own database** for authorization

Explicit Authorization

- Unlike Implicit Authorization, it requires **separate authorization** for each requested resource
- Explicitly maintains authorization for each **requested object**

Notes: ____

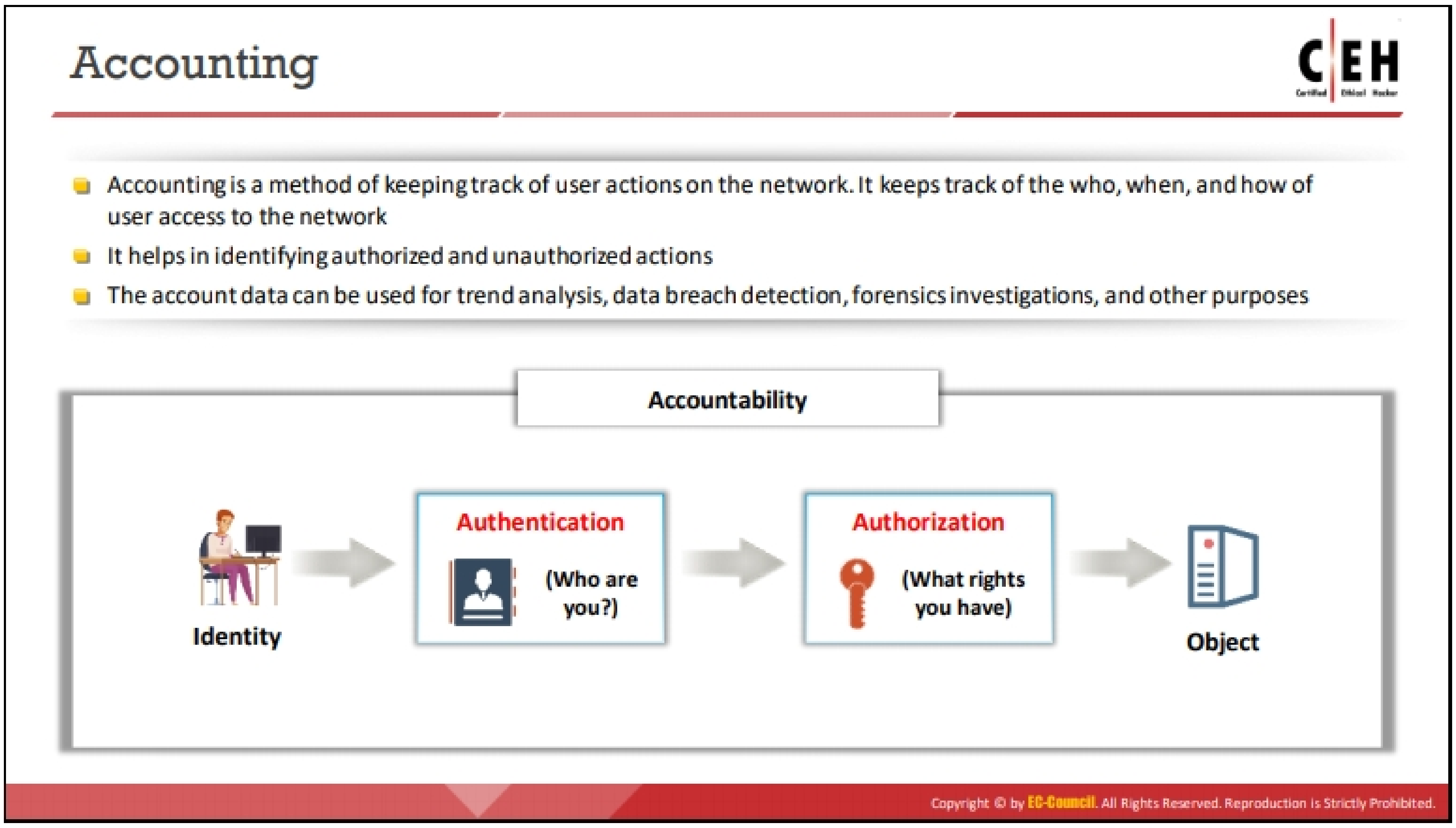
____

____

____

____

____

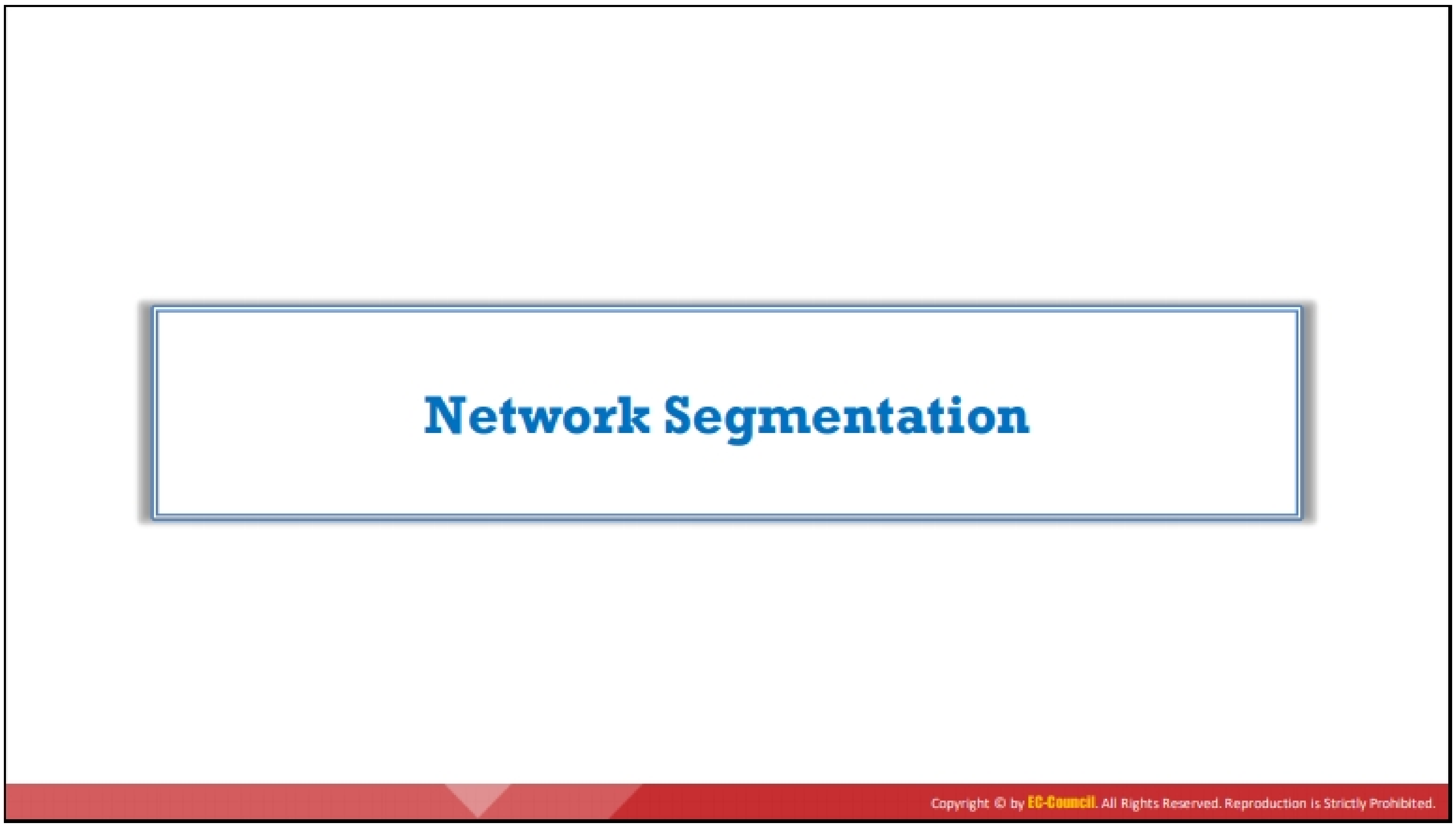


Accounting

- Accounting is a method of keeping track of user actions on the network. It keeps track of the who, when, and how of user access to the network
- It helps in identifying authorized and unauthorized actions
- The account data can be used for trend analysis, data breach detection, forensics investigations, and other purposes

Accountability

Identity → **Authentication** (Who are you?) → **Authorization** (What rights you have) → **Object**

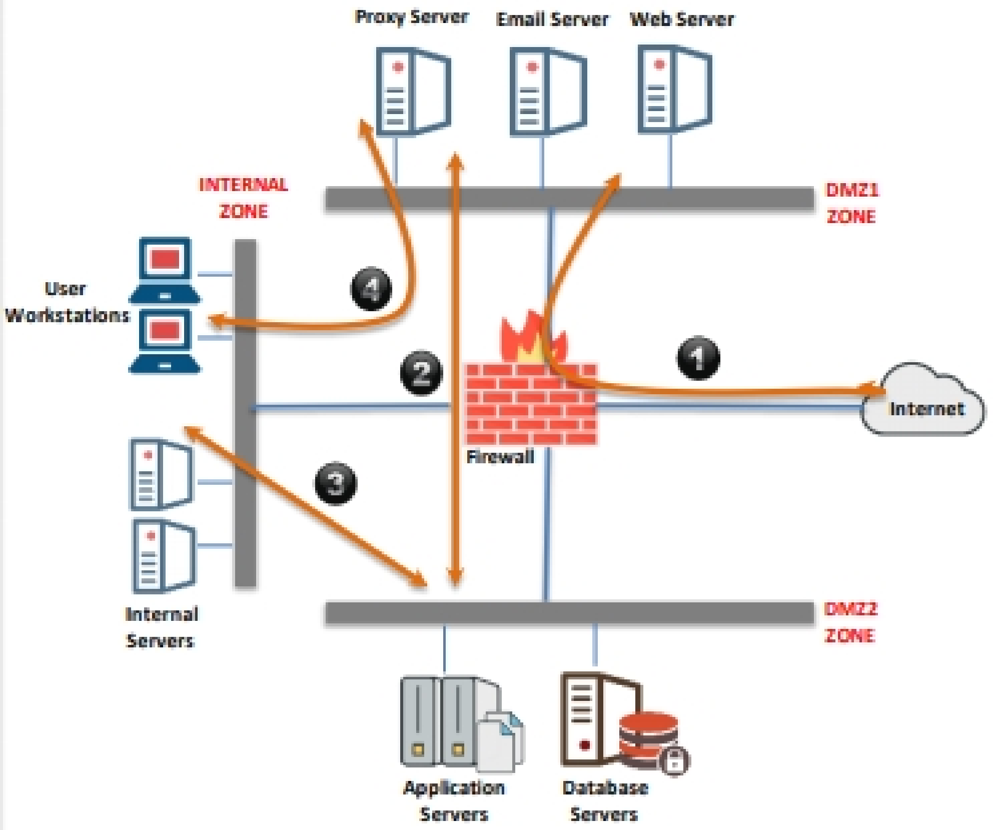


Network Segmentation

Notes:

Network Segmentation

- Network Segmentation is the practice of **splitting** a network into smaller network segments and separating groups of systems or applications from each other
- It defeats the **drawback of the traditional flat network** where all the network resources (such as servers and workstations) are placed on same network. If an attacker can manage to penetrate through perimeter defense, they can see can have easy access to flat network
- In a segmented network, groups of systems or applications that have no interaction with each other will be placed in different network segment
- In such cases, even if an attacker manages to penetrate perimeter security, they can not access to network resources from other segments
- Security benefits of Network Segmentation
  - Improved Security
  - Better Access Control
  - Improved Monitoring
  - Improved Performance
  - Better Containment



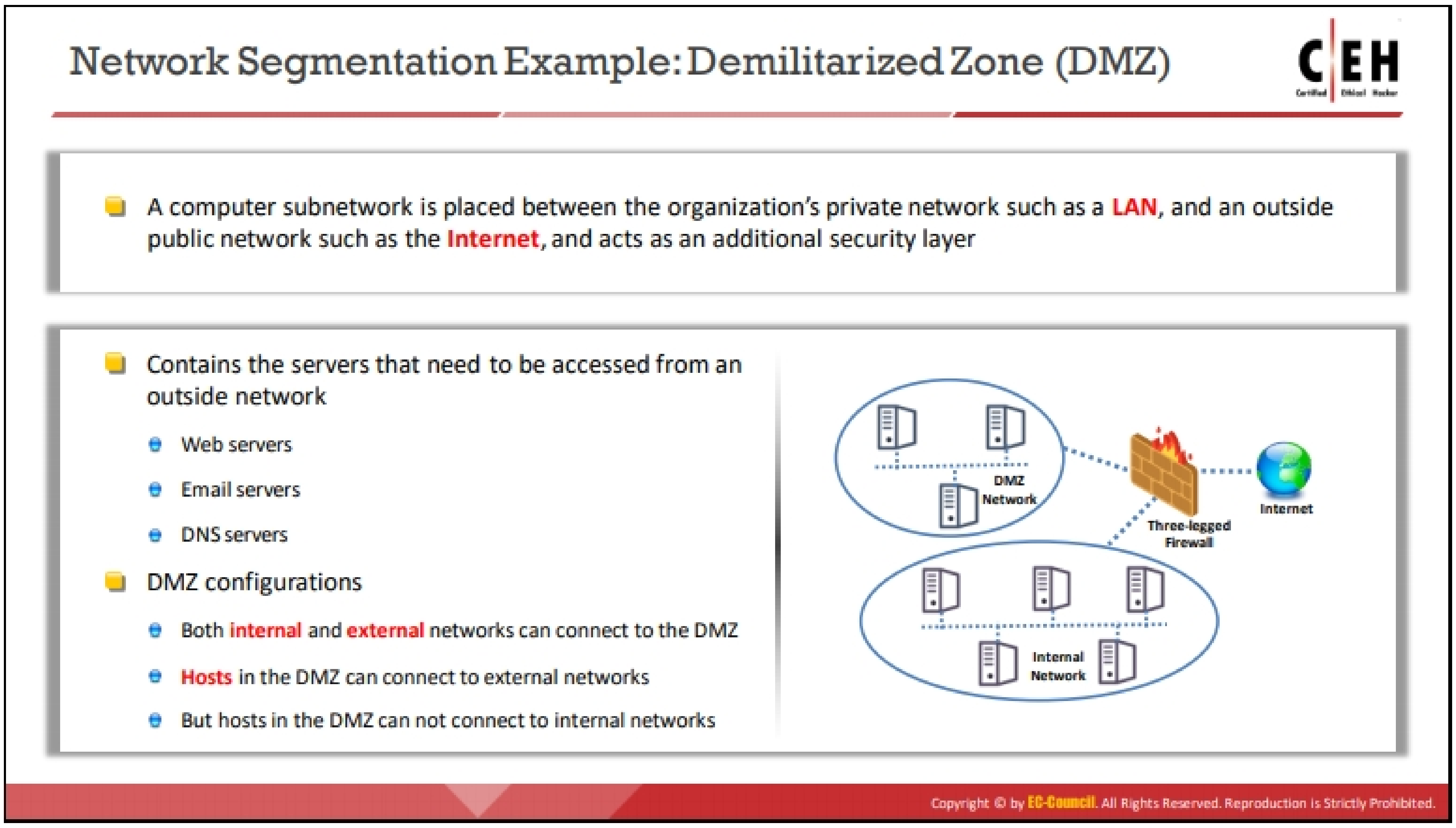
Network Security Zoning

- Network security zoning mechanism allows an organization **to manage a secure network environment** by selecting the appropriate security levels for different **zones of Internet** and **Intranet networks**
- It helps in effectively monitoring and controlling **inbound and outbound traffic**

Examples of Network Security Zones

Internet Zone	An uncontrolled zone **outside the boundaries** of an organization
Internet DMZ	A controlled zone that **provides a barrier** between internal networks and the Internet
Production Network Zone	A restricted zone that strictly **controls direct access** from uncontrolled networks
Intranet Zone	A controlled zone with **no heavy restrictions**
Management Network Zone	A secured zone with **strict policies**

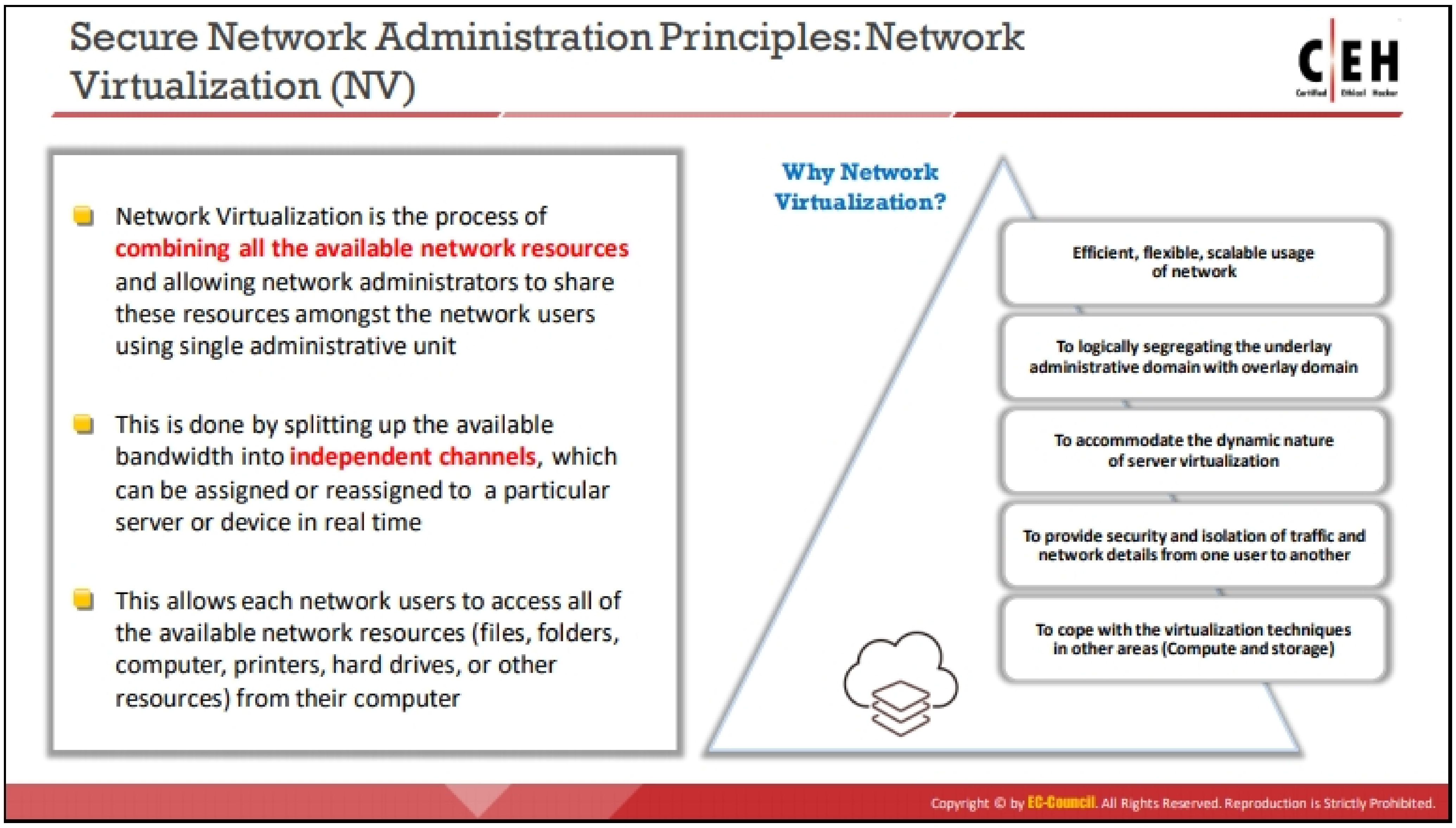
Notes: ____



Network Segmentation Example: Demilitarized Zone (DMZ)

- A computer subnetwork is placed between the organization's private network such as a **LAN**, and an outside public network such as the **Internet**, and acts as an additional security layer

- Contains the servers that need to be accessed from an outside network
  - Web servers
  - Email servers
  - DNS servers
- DMZ configurations
  - Both **internal** and **external** networks can connect to the DMZ
  - **Hosts** in the DMZ can connect to external networks
  - But hosts in the DMZ can not connect to internal networks



Secure Network Administration Principles: Network Virtualization (NV)

- Network Virtualization is the process of **combining all the available network resources** and allowing network administrators to share these resources amongst the network users using single administrative unit

- This is done by splitting up the available bandwidth into **independent channels**, which can be assigned or reassigned to a particular server or device in real time

- This allows each network users to access all of the available network resources (files, folders, computer, printers, hard drives, or other resources) from their computer

Why Network Virtualization?

- Efficient, flexible, scalable usage of network
- To logically segregating the underlay administrative domain with overlay domain
- To accommodate the dynamic nature of server virtualization
- To provide security and isolation of traffic and network details from one user to another
- To cope with the virtualization techniques in other areas (Compute and storage)

Notes: ____

____

____

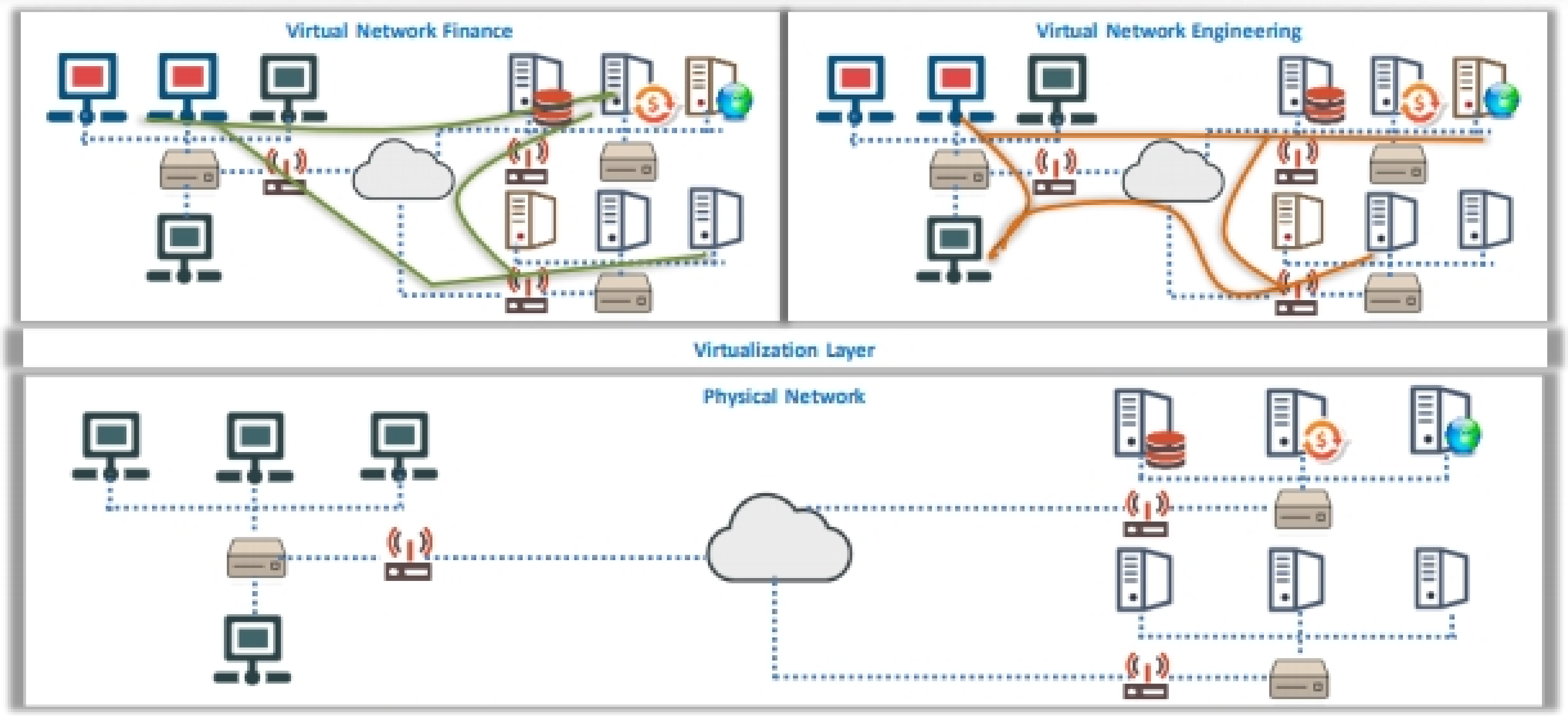
____

____

____

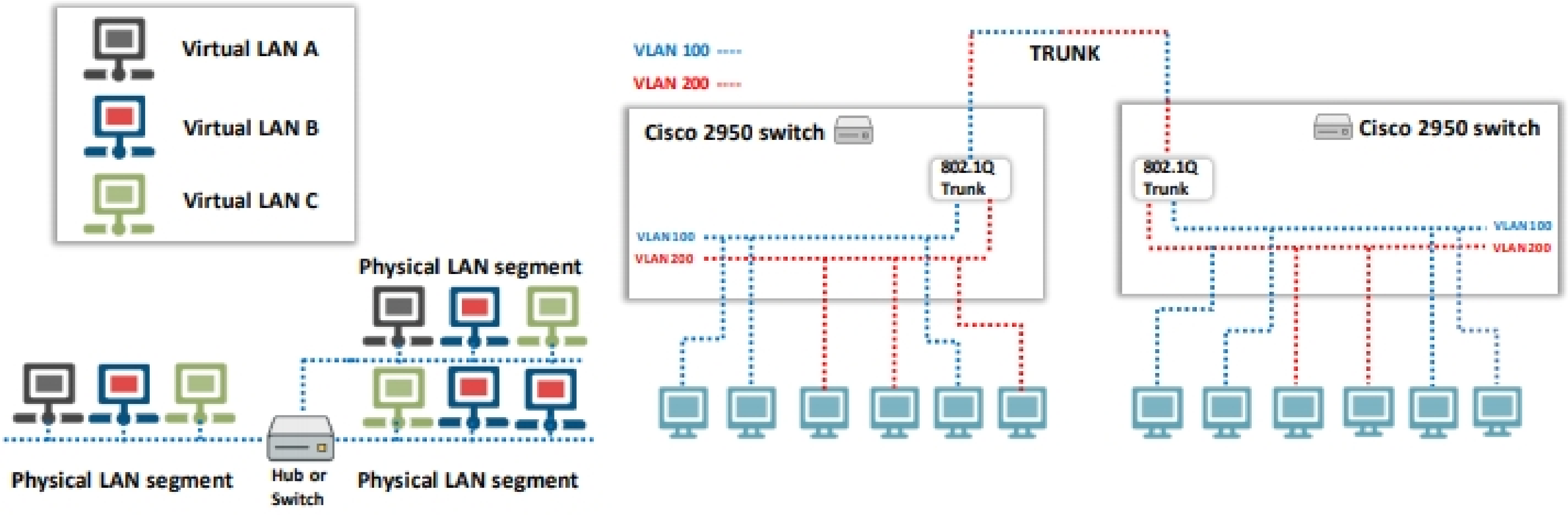
Secure Network Administration Principles: Virtual Networks

- Virtual networks are the **end product of network virtualization**
- Virtual network software is used for virtual networking. This software is either placed outside a virtual server (external) or inside a virtual server, depending on the size and type of the virtualization platform


Virtual Network Finance
Virtual Network Engineering
Virtualization Layer
Physical Network

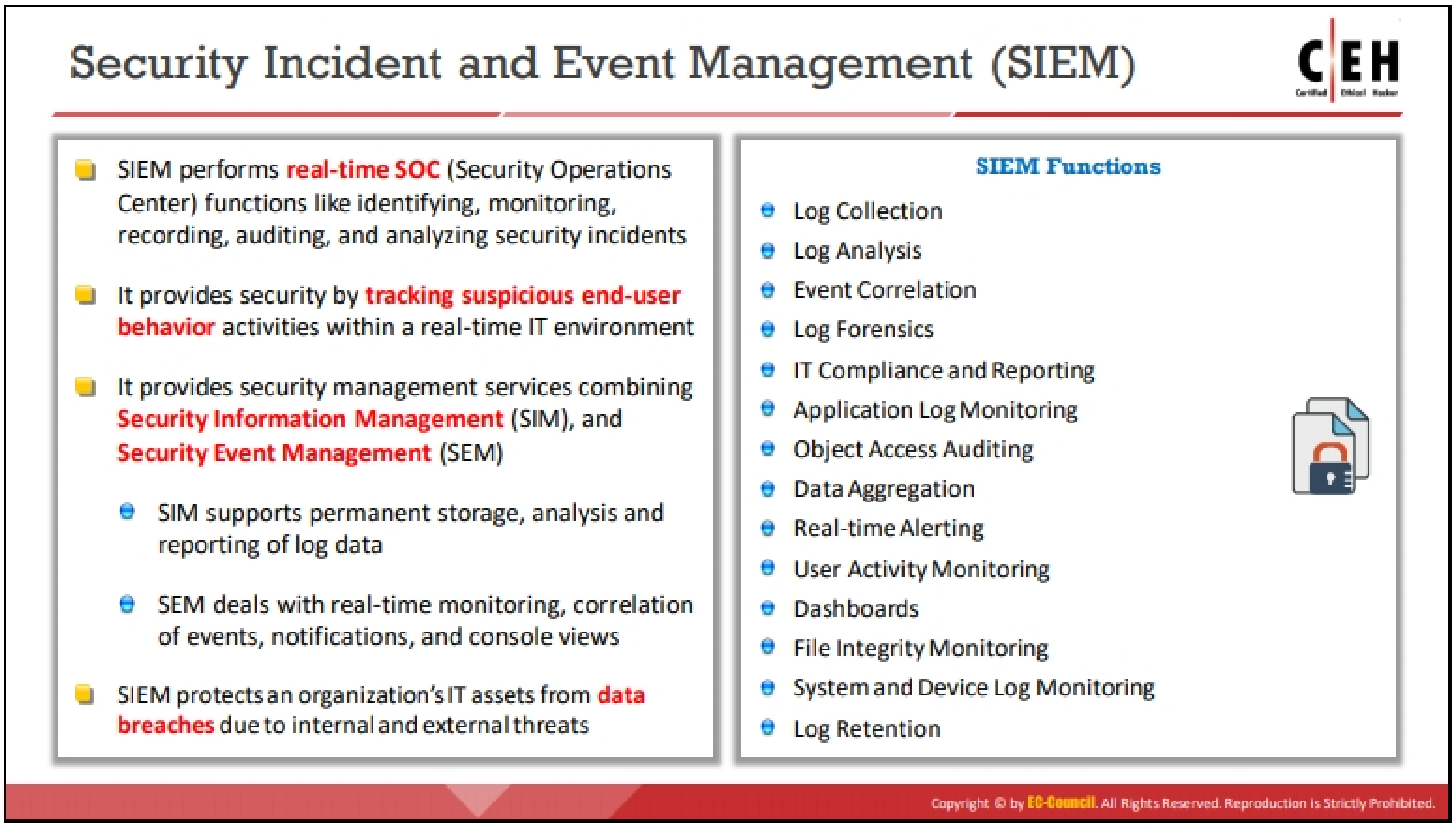
Secure Network Administration Principles: VLANs

- VLANs (Virtual Local Area Networks) are **logical groupings of workstations**, servers, and network devices that behave as if they are on a single, isolated LAN regardless of the location
- The purpose of a VLAN is to create a **simple network with improved security** and better traffic management


Virtual LAN A
Virtual LAN B
Virtual LAN C
Physical LAN segment
Physical LAN segment
Hub or Switch
Physical LAN segment
VLAN 100
VLAN 200
TRUNK
Cisco 2950 switch
802.1Q Trunk
VLAN 100
VLAN 200
Cisco 2950 switch
802.1Q Trunk
VLAN 100
VLAN 200

Notes:

Network Security Solutions



Security Incident and Event Management (SIEM)

- SIEM performs **real-time SOC** (Security Operations Center) functions like identifying, monitoring, recording, auditing, and analyzing security incidents
- It provides security by **tracking suspicious end-user behavior** activities within a real-time IT environment
- It provides security management services combining **Security Information Management** (SIM), and **Security Event Management** (SEM)
  - SIM supports permanent storage, analysis and reporting of log data
  - SEM deals with real-time monitoring, correlation of events, notifications, and console views
- SIEM protects an organization's IT assets from **data breaches** due to internal and external threats

SIEM Functions

- Log Collection
- Log Analysis
- Event Correlation
- Log Forensics
- IT Compliance and Reporting
- Application Log Monitoring
- Object Access Auditing
- Data Aggregation
- Real-time Alerting
- User Activity Monitoring
- Dashboards
- File Integrity Monitoring
- System and Device Log Monitoring
- Log Retention

Notes: ____

____

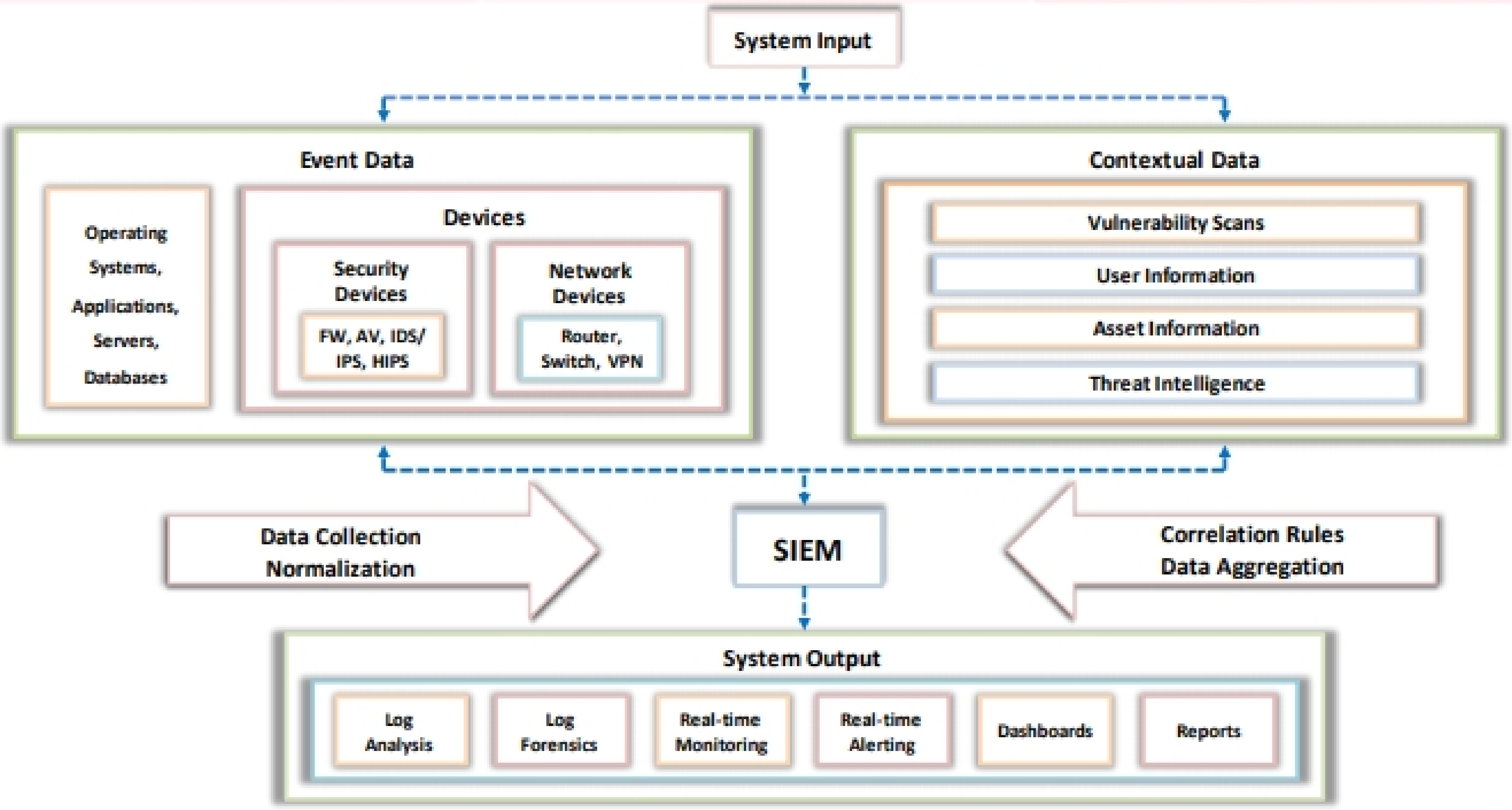
____

____

____

____

SIEM Architecture



System Input

Event Data

Operating Systems, Applications, Servers, Databases

Devices

Security Devices

FW, AV, IDS/IPS, HIPS

Network Devices

Router, Switch, VPN

Contextual Data

Vulnerability Scans

User Information

Asset Information

Threat Intelligence

Data Collection
Normalization

SIEM

Correlation Rules
Data Aggregation

System Output

Log Analysis

Log Forensics

Real-time Monitoring

Real-time Alerting

Dashboards

Reports

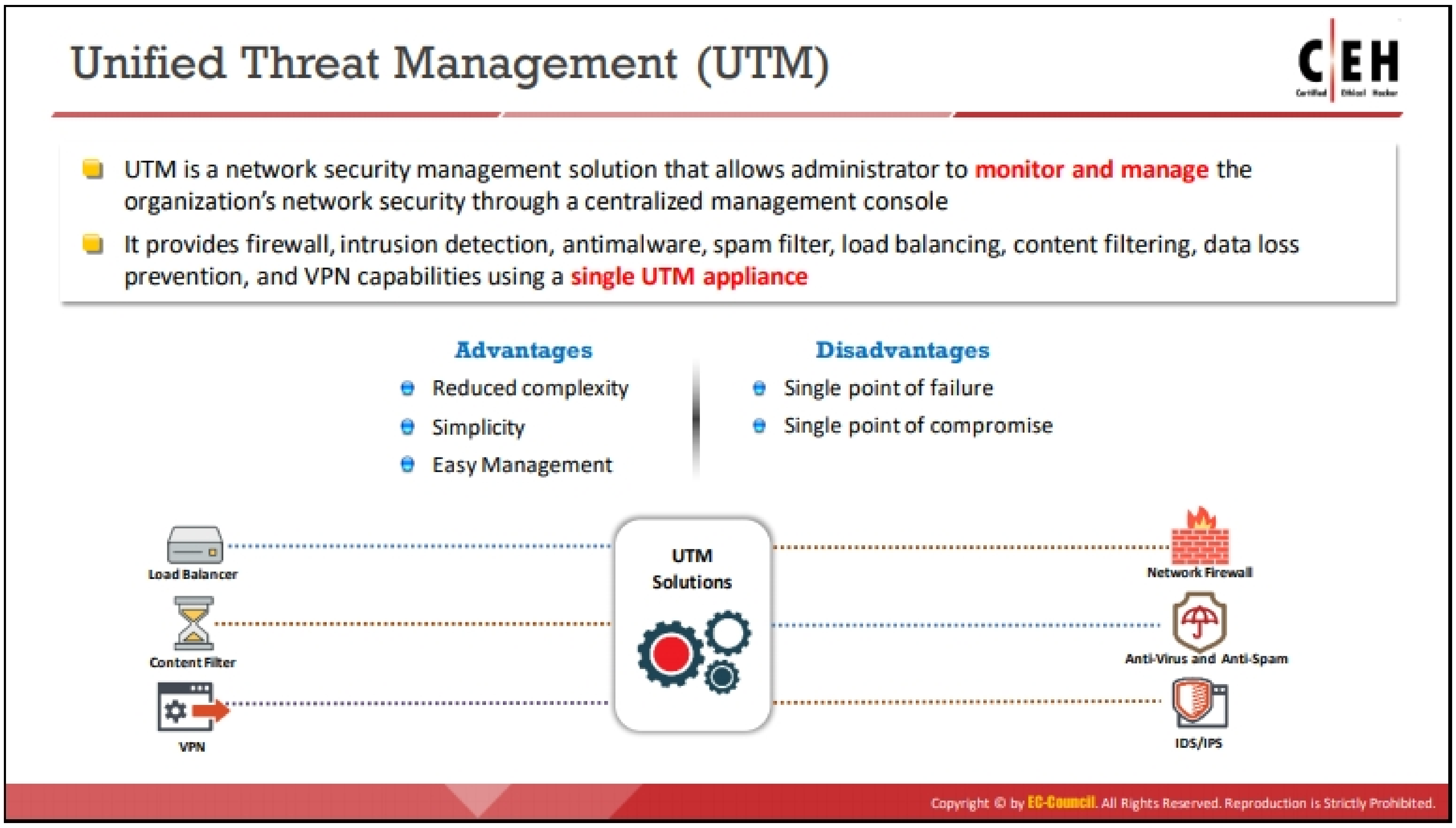
User Behavior Analytics (UBA)

- UBA is the process of **tracking user behavior** to detect malicious attacks, potential threats, and financial fraud
- It provides **advanced threat detection** in an organization to monitor specific behavioral characteristics of employees
- UBA technologies are designed to **identify variations** in **traffic patterns** caused by user behaviors which can be either disgruntled employees or malicious attackers

Why User Behavior Analytics is Effective?

- Analyzes different patterns of human behavior and large volumes of user data
- Monitors geolocation for each login attempt
- Detects malicious behavior and reduces risk
- Monitors privileged accounts and gives real time alerts for suspicious behavior
- Provides insights to security teams
- Produces results soon after deployment

Notes:

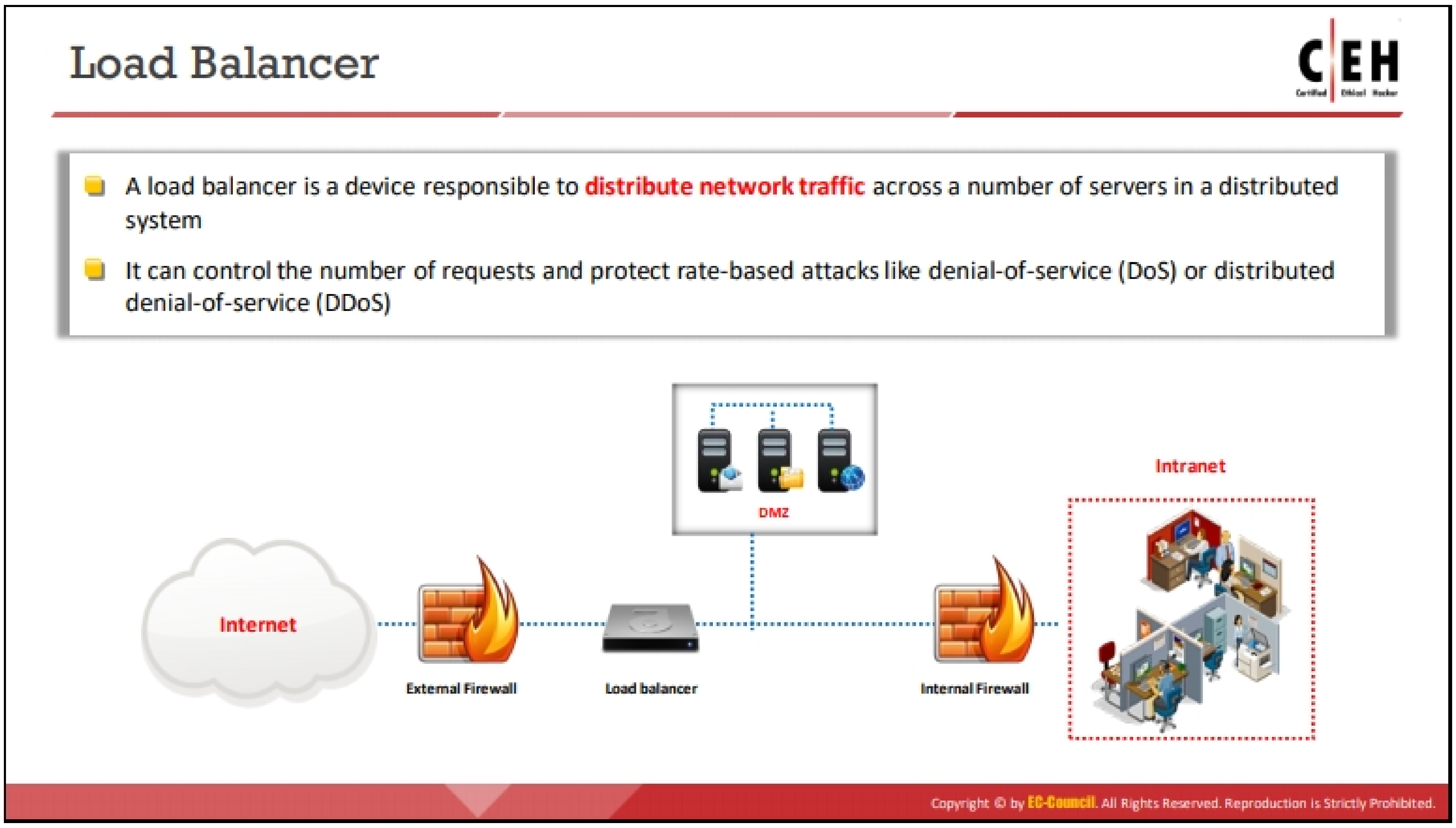


Unified Threat Management (UTM)

- UTM is a network security management solution that allows administrator to **monitor and manage** the organization's network security through a centralized management console
- It provides firewall, intrusion detection, antimalware, spam filter, load balancing, content filtering, data loss prevention, and VPN capabilities using a **single UTM appliance**

Advantages	Disadvantages
Reduced complexity	Single point of failure
Simplicity	Single point of compromise
Easy Management	

Load Balancer
Content Filter
VPN
UTM Solutions
Network Firewall
Anti-Virus and Anti-Spam
IDS/IPS



Load Balancer

- A load balancer is a device responsible to **distribute network traffic** across a number of servers in a distributed system
- It can control the number of requests and protect rate-based attacks like denial-of-service (DoS) or distributed denial-of-service (DDoS)

DMZ
Intranet
Internet
External Firewall
Load balancer
Internal Firewall

Notes: ____

____

____

____

____

____

Network Access Control (NAC)

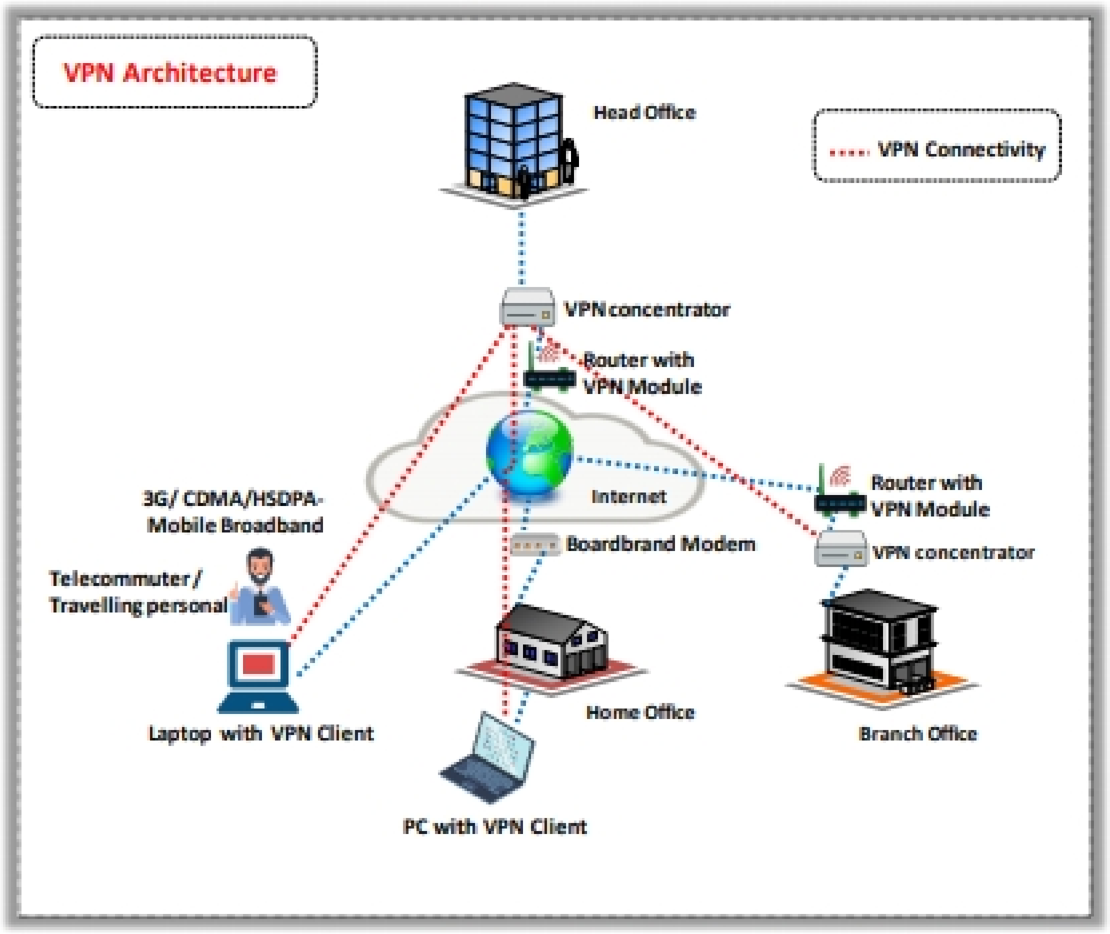
- Network Access Control, also known as Network Admission Control (NAC), are appliances or solutions that attempt to protect the network by **restricting the connection** of an end user to the network based upon a security policy
- The **pre-installed software agent** may inspect several items before admitting the device and may restrict where the device is connected

What NAC does?

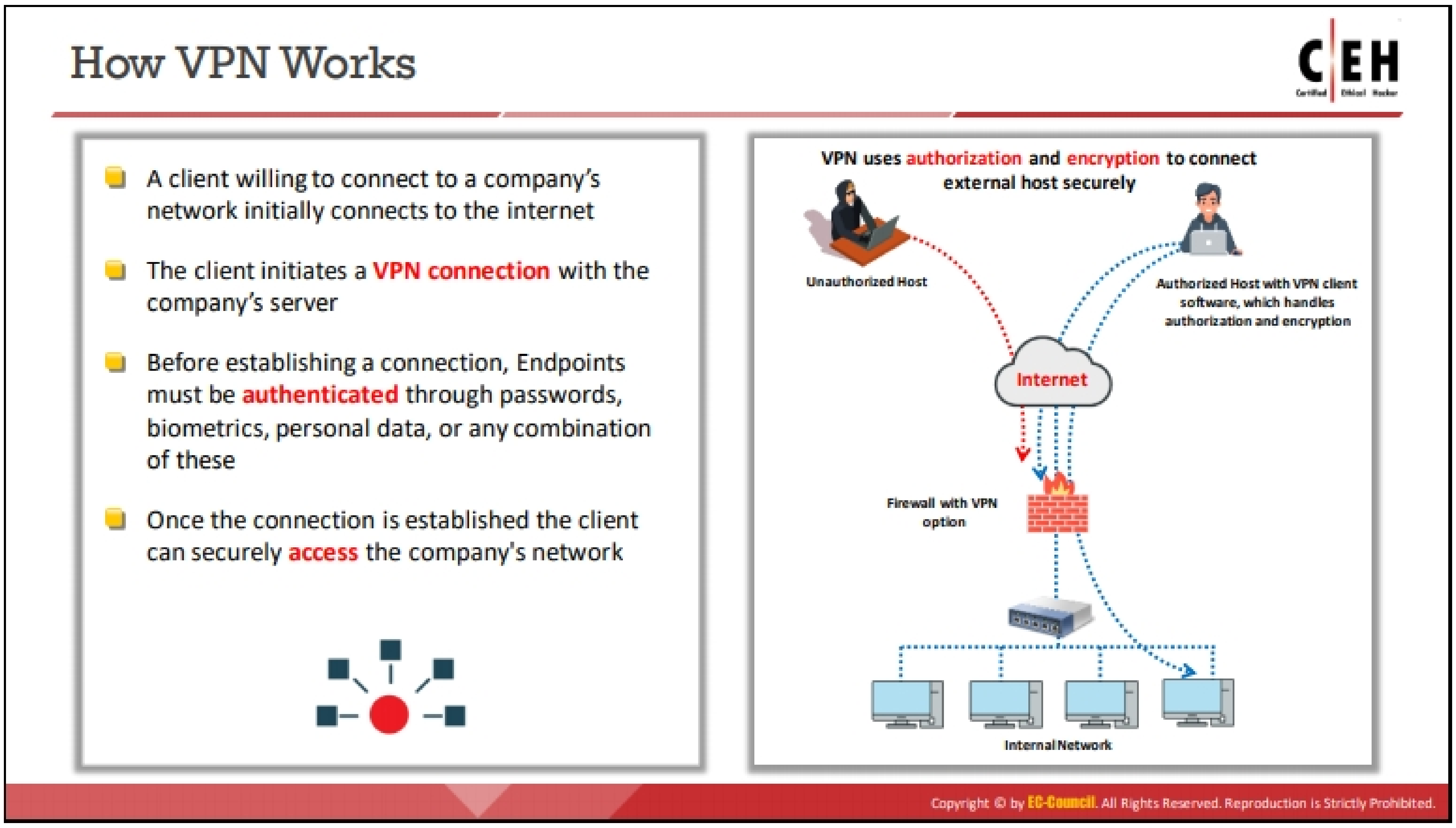
- Authenticate users connected to network resources
- Identify devices, platforms, and operating systems
- Define a connection point for network devices
- Develop and apply security policies

Virtual Private Network (VPN)

- VPNs are used to **securely communicate** with different computers over insecure channels
- A VPN use the Internet and ensures secure communication to distant offices or users within the **enterprise's network**


VPN Architecture
Head Office
VPN Connectivity
VPN concentrator
Router with VPN Module
Internet
3G/ CDMA/HSDPA-Mobile Broadband
Boardbrand Modem
Router with VPN Module
VPN concentrator
Telecommuter / Travelling personal
Laptop with VPN Client
Home Office
Branch Office
PC with VPN Client

Notes:

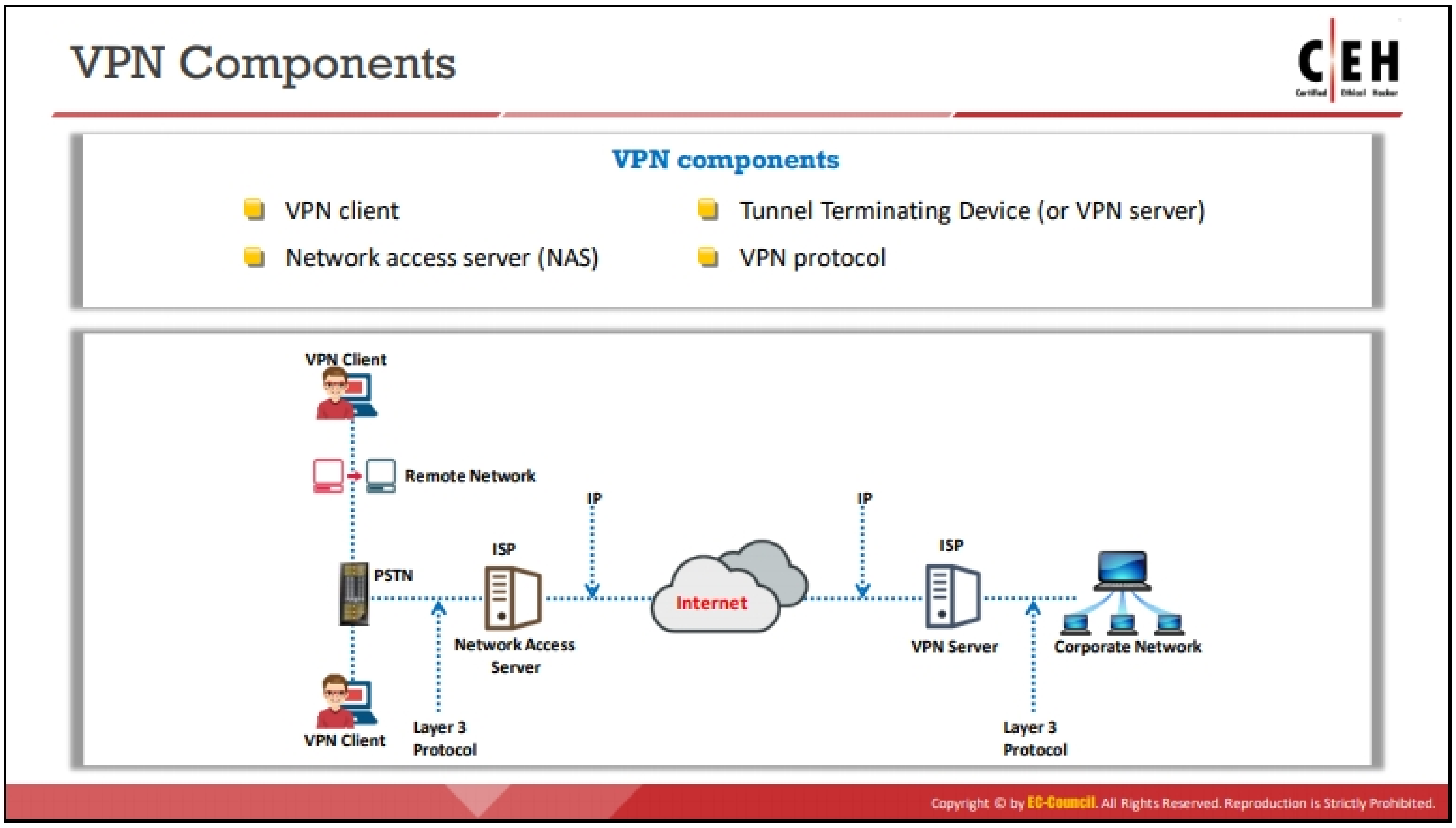


How VPN Works

- A client willing to connect to a company's network initially connects to the internet
- The client initiates a **VPN connection** with the company's server
- Before establishing a connection, Endpoints must be **authenticated** through passwords, biometrics, personal data, or any combination of these
- Once the connection is established the client can securely **access** the company's network

VPN uses **authorization** and **encryption** to connect external host securely

Unauthorized Host
Authorized Host with VPN client software, which handles authorization and encryption
Internet
Firewall with VPN option
Internal Network



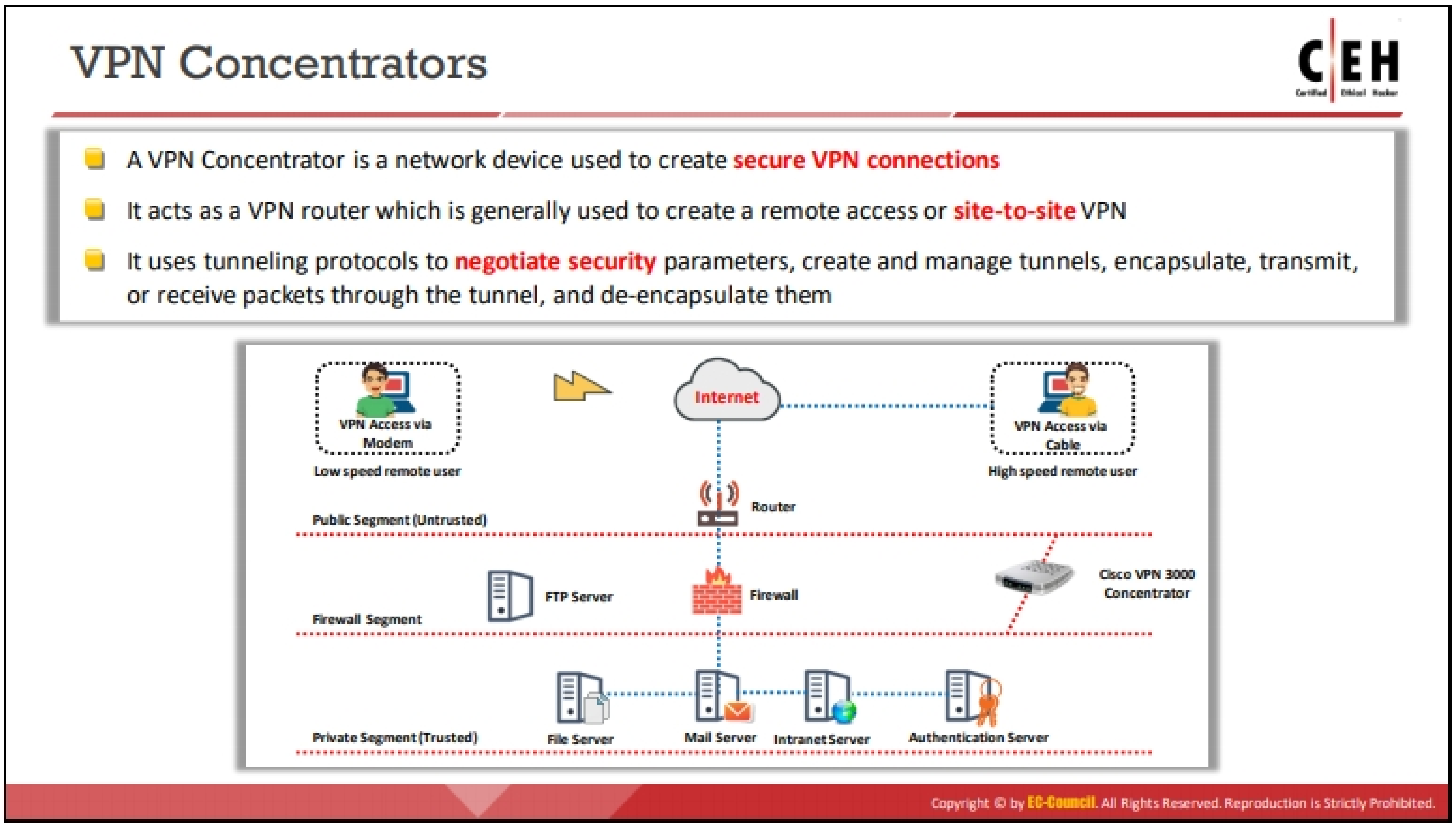
VPN Components

VPN components

- VPN client
- Network access server (NAS)
- Tunnel Terminating Device (or VPN server)
- VPN protocol

VPN Client
Remote Network
PSTN
ISP
Network Access Server
IP
Internet
IP
ISP
VPN Server
Corporate Network
VPN Client
Layer 3 Protocol
Layer 3 Protocol

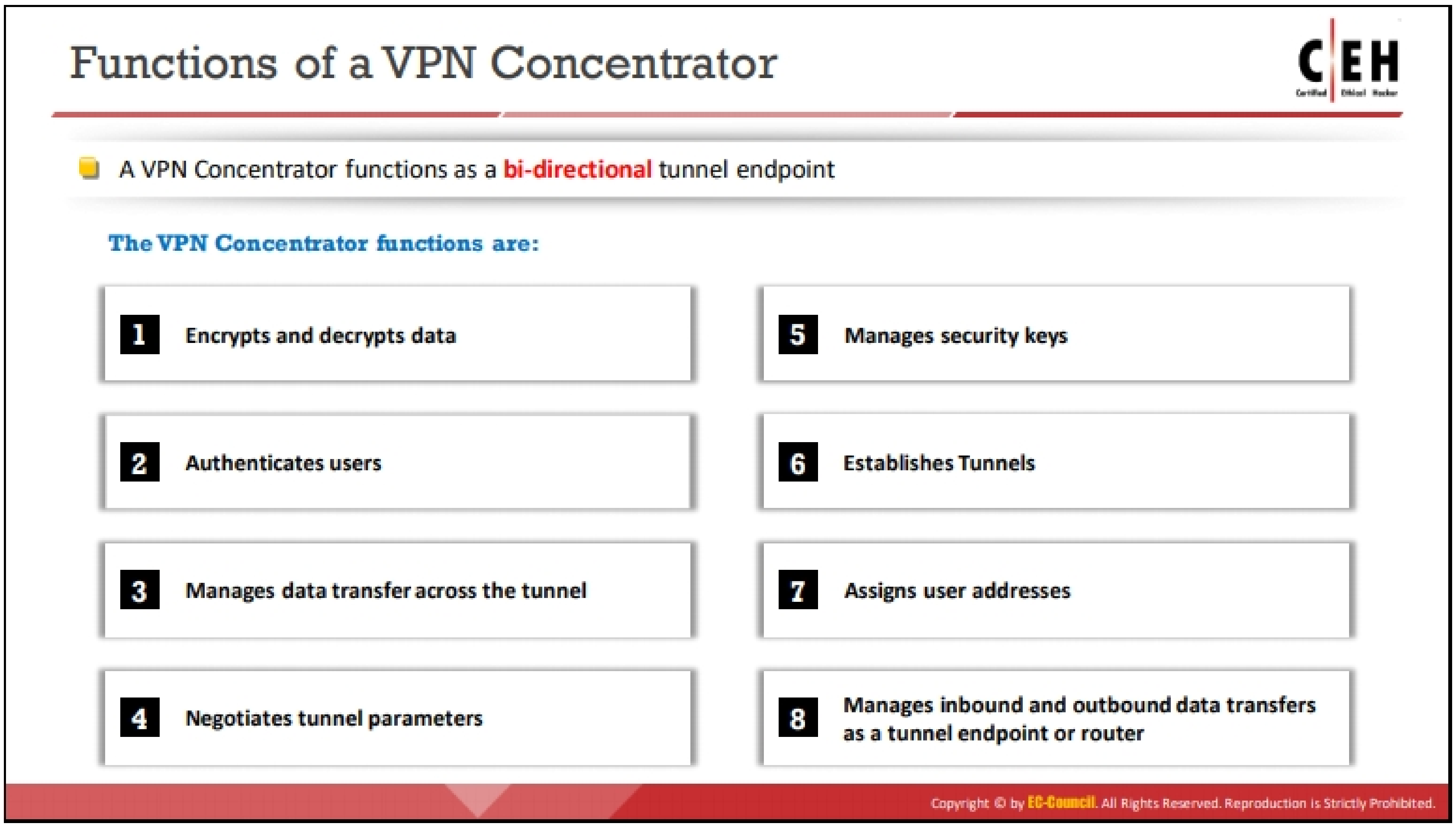
Notes:



VPN Concentrators

- A VPN Concentrator is a network device used to create **secure VPN connections**
- It acts as a VPN router which is generally used to create a remote access or **site-to-site** VPN
- It uses tunneling protocols to **negotiate security** parameters, create and manage tunnels, encapsulate, transmit, or receive packets through the tunnel, and de-encapsulate them

VPN Access via Modem
Low speed remote user
Internet
VPN Access via Cable
High speed remote user
Router
Public Segment (Untrusted)
FTP Server
Firewall
Cisco VPN 3000 Concentrator
Firewall Segment
File Server
Mail Server
Intranet Server
Authentication Server
Private Segment (Trusted)



Functions of a VPN Concentrator

- A VPN Concentrator functions as a **bi-directional** tunnel endpoint

The VPN Concentrator functions are:

1. Encrypts and decrypts data
2. Authenticates users
3. Manages data transfer across the tunnel
4. Negotiates tunnel parameters
5. Manages security keys
6. Establishes Tunnels
7. Assigns user addresses
8. Manages inbound and outbound data transfers as a tunnel endpoint or router

Notes: ____

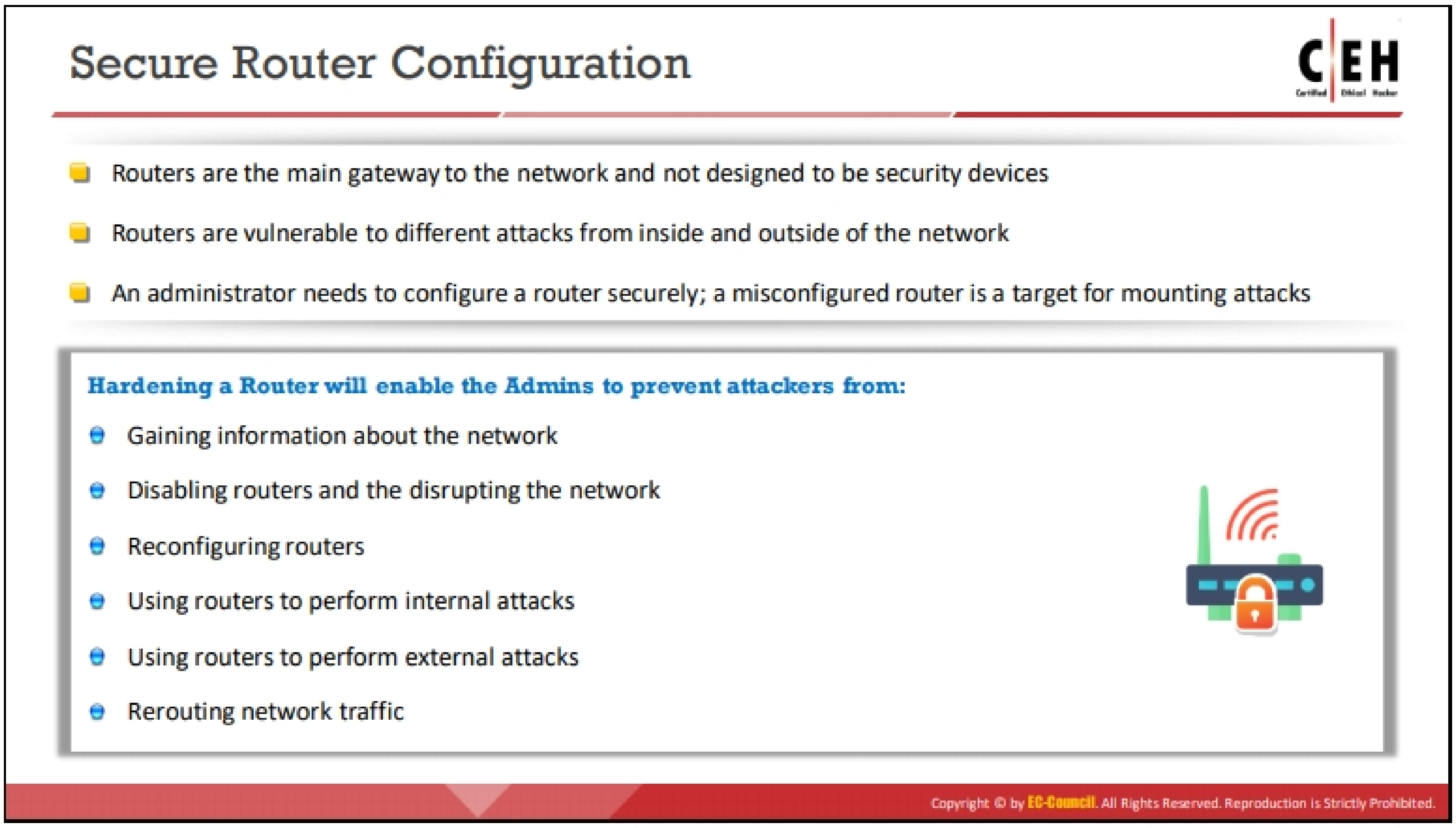
____

____

____

____

____



Secure Router Configuration

- Routers are the main gateway to the network and not designed to be security devices
- Routers are vulnerable to different attacks from inside and outside of the network
- An administrator needs to configure a router securely; a misconfigured router is a target for mounting attacks

Hardening a Router will enable the Admins to prevent attackers from:

- Gaining information about the network
- Disabling routers and the disrupting the network
- Reconfiguring routers
- Using routers to perform internal attacks
- Using routers to perform external attacks
- Rerouting network traffic

Router Security Measures

1. Implement written, approved, and distributed router policy
2. Returned IOS version should be checked and up-to-date
3. Configure users and passwords
4. Enable password encryption
5. Implement access restriction on console
6. Disable unnecessary services
7. Properly configure necessary services such as DNS
8. Shutdown unnecessary interfaces
9. Identify and check the ports and protocols
10. Implement ACL to limit traffic to the required ports and protocols
11. Implement ACL to block reserved and inappropriate addresses
12. Enable logging
13. Use NTP, to set the router's time of day accurately
14. Logs checked, reviewed, and archived as per defined policy

Notes: ____

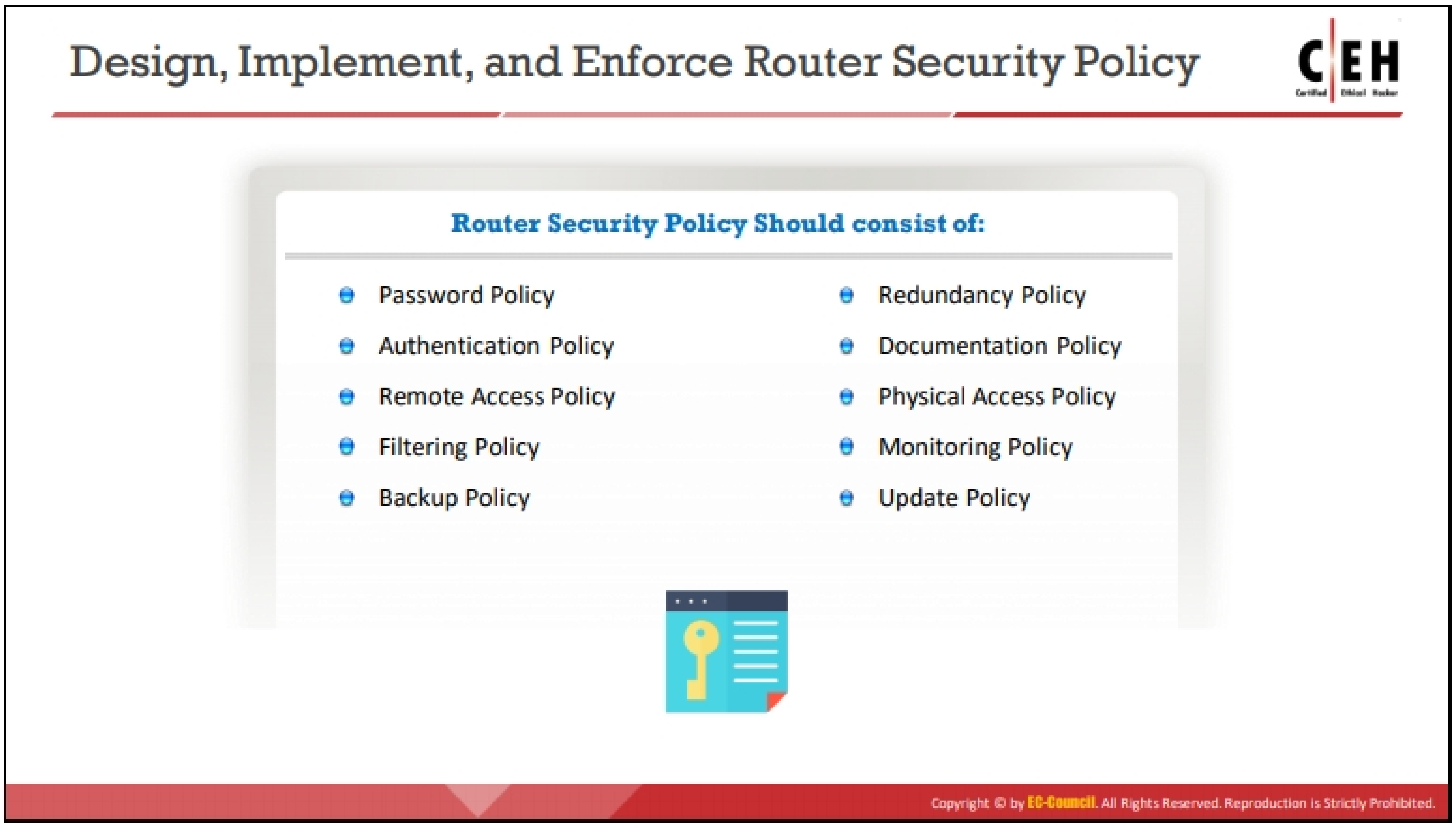
____

____

____

____

____



Design, Implement, and Enforce Router Security Policy

Router Security Policy Should consist of:

- Password Policy
- Authentication Policy
- Remote Access Policy
- Filtering Policy
- Backup Policy
- Redundancy Policy
- Documentation Policy
- Physical Access Policy
- Monitoring Policy
- Update Policy

Data Leakage

Notes:

Data Leakage

- Data leakage refers to unauthorized access or disclosure of **sensitive or confidential data**
- Data leakage may happen electronically through an email or malicious link or via some physical method such as device theft or hacker break-ins

Major Risks to Organizations

- Loss of customer loyalty
- Potential litigations
- Heavy fines
- Decline in share value
- Loss of brand name
- Loss of reputation
- Reduction of sales and revenue
- Unfavorable media attention
- Unfavorable competitor advantage
- Insolvency or liquidation
- Loss of new and existing customers
- Monetary loss
- Prone to cyber criminal attacks
- Loss of productivity
- Disclosure of trade secrets
- Pre-release of latest technology developed by company
- Loss of proprietary and customer information
- Ready to release projects get pirated

Data Leakage Threats

Insider Threats

- Disgruntled or negligent employees may knowingly or unknowingly leak sensitive data to the outside world, incurring huge **financial losses** and business interruptions
- Employees may use various techniques such as eavesdropping, shoulder surfing, or dumpster diving, to gain unauthorized **access** to information in violation of **corporate policies**

Reasons for Insider Threats

- Inadequate security **awareness** and **training**
- Lack of proper management controls for **monitoring employee activities**
- Use of an insecure mode of data **transfers**

External Threats

- Attackers take advantage of insiders' vulnerabilities to perform various attacks by **stealing the credentials** of a legitimate employee
- This gives the attacker unlimited **access to the target network**

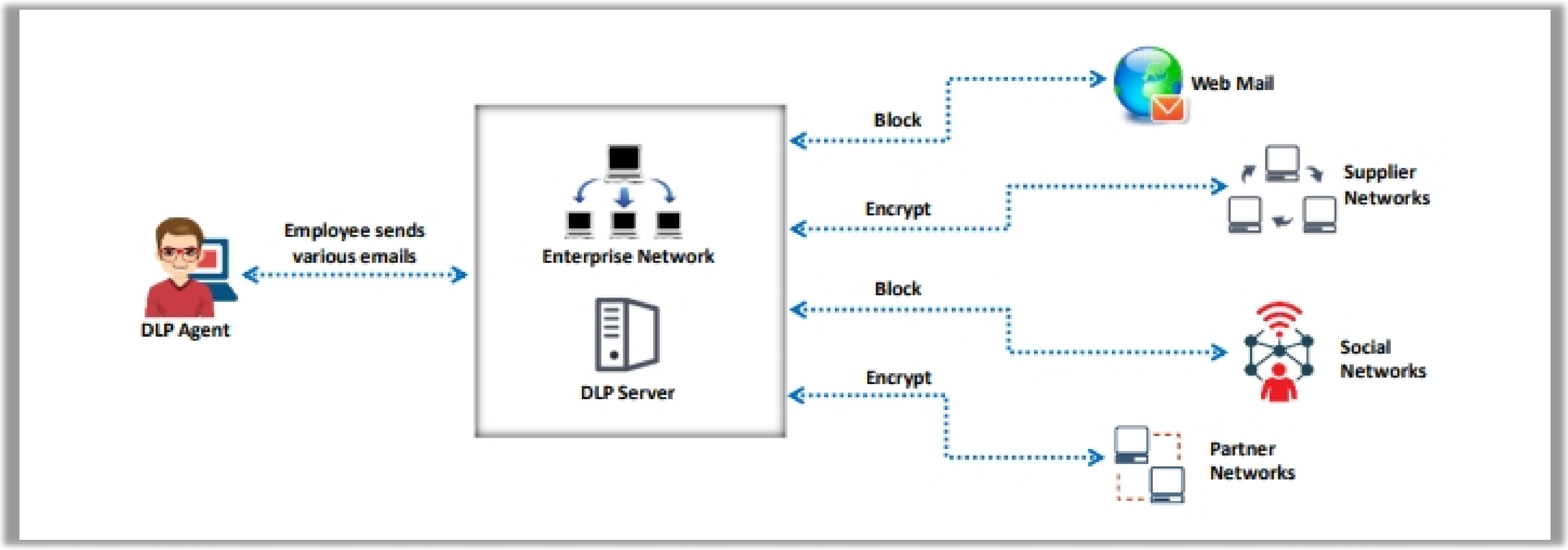
Examples of External Threats

- Hacking or Code Injection Attacks
- Malware
- Phishing
- Corporate Espionage or Competitors
- Business Partners or Contractors

Notes:

What is Data Loss Prevention (DLP)?

- DLP is the identification and **monitoring of sensitive data** to ensure that end users do not send sensitive information outside the corporate network


DLP Agent
Employee sends various emails
Enterprise Network
DLP Server
Block
Web Mail
Encrypt
Supplier Networks
Block
Social Networks
Encrypt
Partner Networks

Data Backup

Notes: ______________________________

Data Backup

- Data is the **heart** of any organization; data loss can be costly as it may have financial impact to any organization
- Backup is the process of making a **duplicate copy** of critical data that can be used for restore and recovery purposes when the primary copy is lost or corrupted either accidentally or on purpose
- Data backup plays a **crucial role** in maintaining business continuity by helping organizations recover from IT disasters such as hardware failures, application failures, security breaches, human error, and deliberate sabotage

Backup Strategy or Plan

- Identify critical **business data**
- Select **backup media**
- Select **backup technology**
- Select appropriate **RAID levels**
- Select an **appropriate backup** method
- Choose the **backup location**
- Select the **backup types**
- Choose the **right backup** solution
- Conduct a recovery **drill test**

RAID (Redundant Array Of Independent Disks) Technology

- RAID is a method of combining multiple hard drives into a single unit and writing data across several disk drives that offers **fault tolerance** (if one drive fails, the system can continue operations)
- Placing data on **RAID disks** enables input/output (I/O) operations to overlap in a balanced way, improving system performance, simplifying the storage management, and protecting from data loss
- RAID represents a portion of computer storage that can divide and replicate data among several drives working as **secondary storage**
- RAID has six levels: RAID 0, RAID 1, RAID 3, RAID 5, RAID 10, and RAID 50, to function effectively. All the RAID levels depend on the below storage techniques:
  - Striping
  - Mirroring
  - Parity

Notes: ____

Advantages and Disadvantages of RAID Systems

Advantages

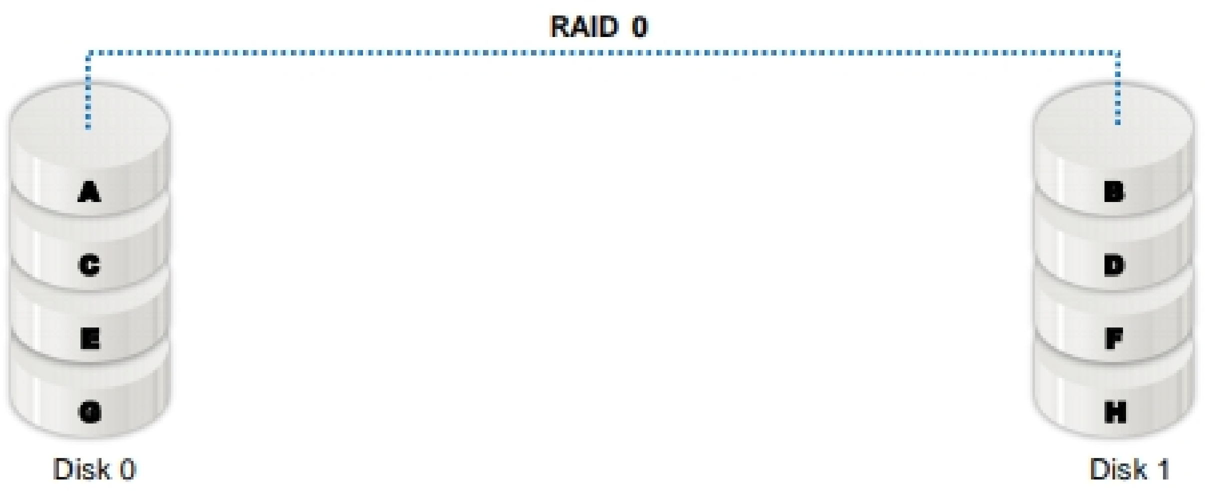
- RAID offers **hot-swapping** or **hot plugging** i.e. system component replacement (in case a drive fails) without affecting **network functionality**
- RAID supports **disk striping**, resulting in an improvement of read/write performance as the system completely utilizes the processor speed
- Increased RAID **parity checks** prevent a system crash or data loss
- Increased data **redundancy** helps restore data in the event of a drive failure
- RAID increases **system uptime**

Disadvantages

- RAID is not compatible with some **hardware** components and **software** systems e.g., system imaging programs
- RAID data is **lost** if important drives fail one after another e.g., in the case of RAID 5, a drive that is exclusive for parity cannot recreate the first drive if a second drive fails too
- RAID cannot protect data and offer performance boosts for all applications
- RAID **configuration** is difficult

RAID Level 0: Disk Striping

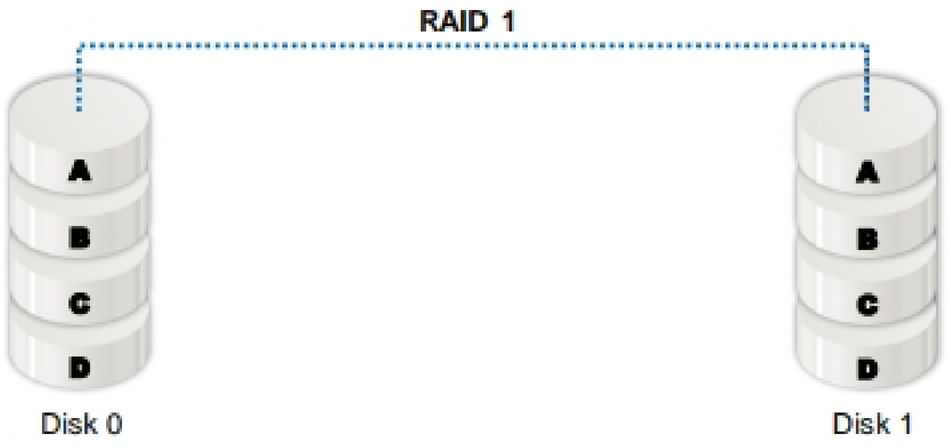
- RAID Level 0 splits data into blocks and written evenly across **multiple hard drives**
- Disk Striping improves I/O performance by spreading the **I/O load** across many channels and disk drives
- Data recovery **is not possible** if a drive fails
- It requires a minimum of **two drives**
- It does not provide **data redundancy**



Notes: ____

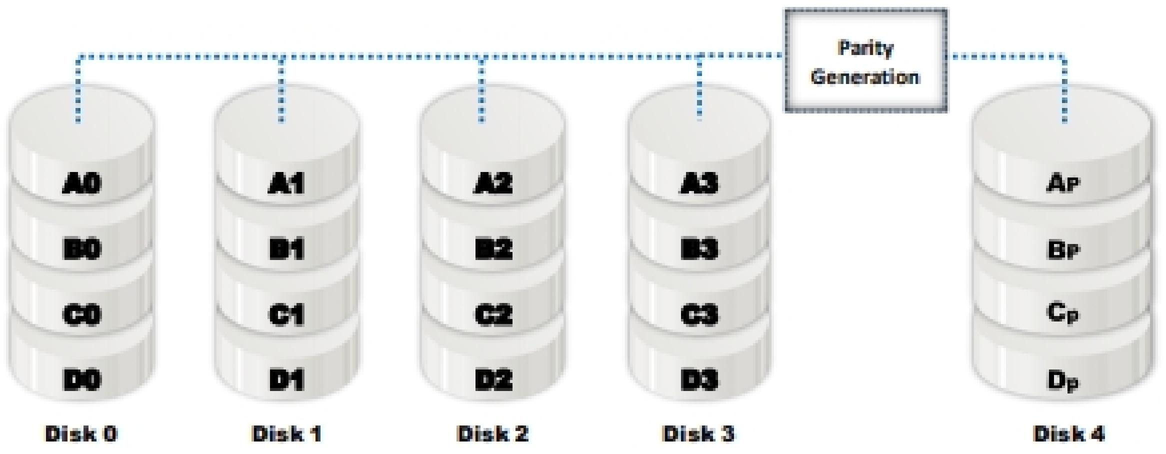
RAID Level 1: Disk Mirroring

- Multiple copies of data are simultaneously written to **multiple drives**
- Provides data redundancy by **duplicating the drive data** to multiple drives
- If one drive fails, **data recovery** is possible
- Requires a minimum of **two drives**

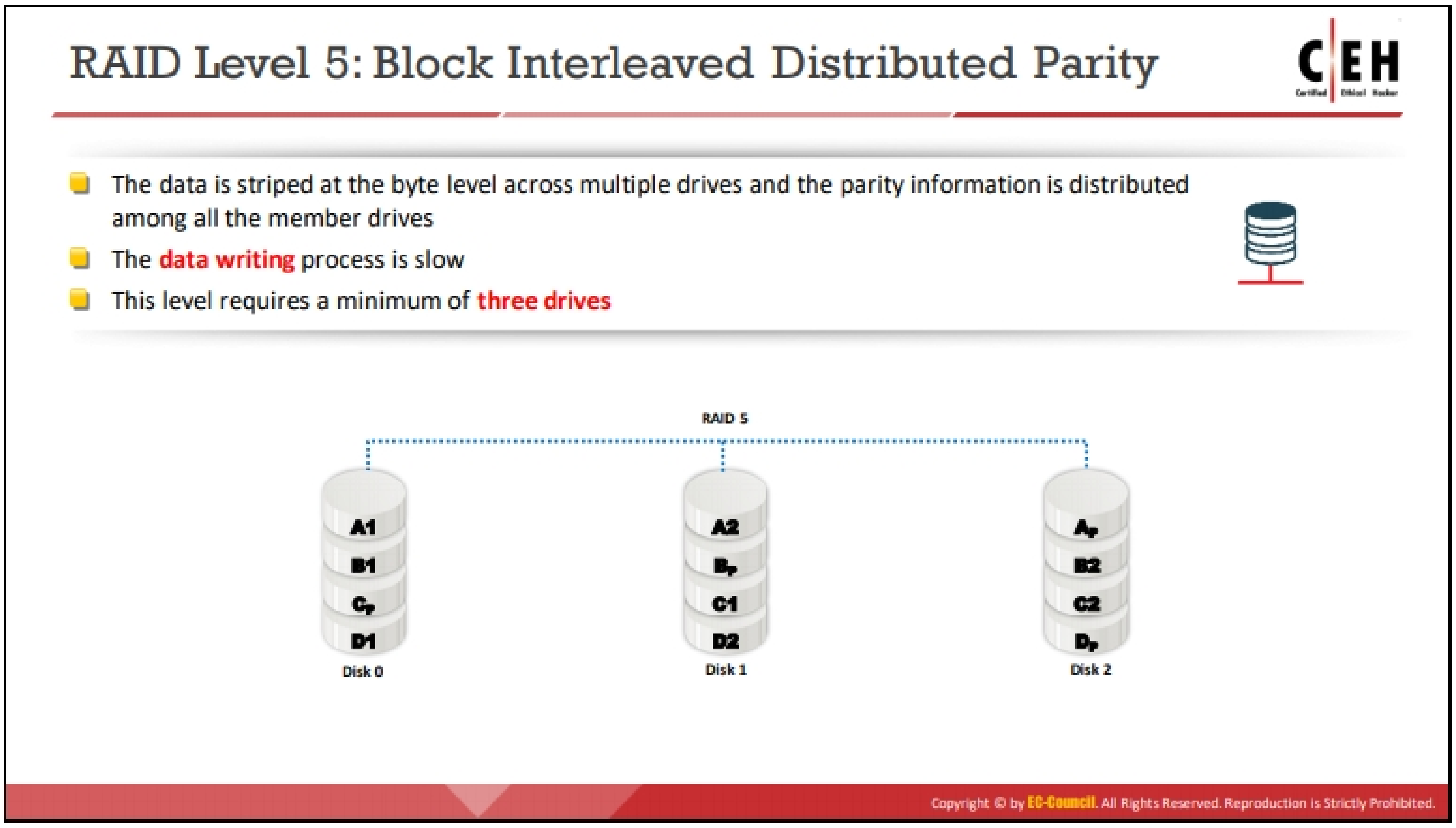

RAID 1
A
B
C
D
Disk 0
A
B
C
D
Disk 1

RAID Level 3: Disk Striping with Parity

- Data is striped at the **byte level** across multiple drives. One drive per set is taken up for parity information
- If a drive fails, **data recovery and error correction** are possible using the parity drive in the set
- The **parity drive** stores the information on multiple drives


Parity Generation
A0
B0
C0
D0
Disk 0
A1
B1
C1
D1
Disk 1
A2
B2
C2
D2
Disk 2
A3
B3
C3
D3
Disk 3
Ap
Bp
Cp
Dp
Disk 4

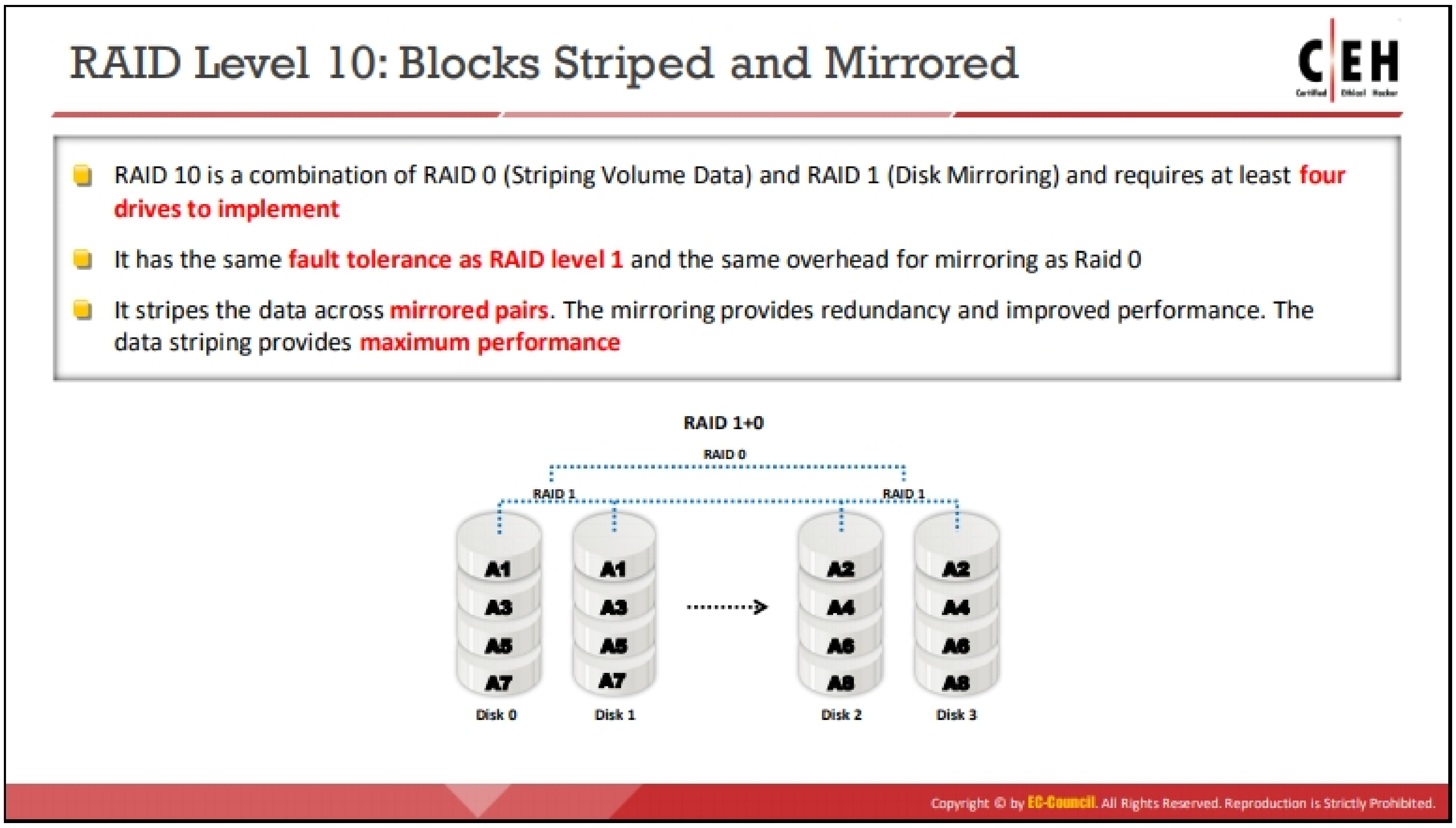
Notes: ____



RAID Level 5: Block Interleaved Distributed Parity

- The data is striped at the byte level across multiple drives and the parity information is distributed among all the member drives
- The **data writing** process is slow
- This level requires a minimum of **three drives**

RAID 5
A1
B1
Cp
D1
Disk 0
A2
Bp
C1
D2
Disk 1
Ap
B2
C2
Dp
Disk 2



RAID Level 10: Blocks Striped and Mirrored

- RAID 10 is a combination of RAID 0 (Striping Volume Data) and RAID 1 (Disk Mirroring) and requires at least **four drives to implement**
- It has the same **fault tolerance as RAID level 1** and the same overhead for mirroring as Raid 0
- It stripes the data across **mirrored pairs**. The mirroring provides redundancy and improved performance. The data striping provides **maximum performance**

RAID 1+0
RAID 0
RAID 1
RAID 1
A1
A3
A5
A7
Disk 0
A1
A3
A5
A7
Disk 1
A2
A4
A6
A8
Disk 2
A2
A4
A6
A8
Disk 3

Notes: ____

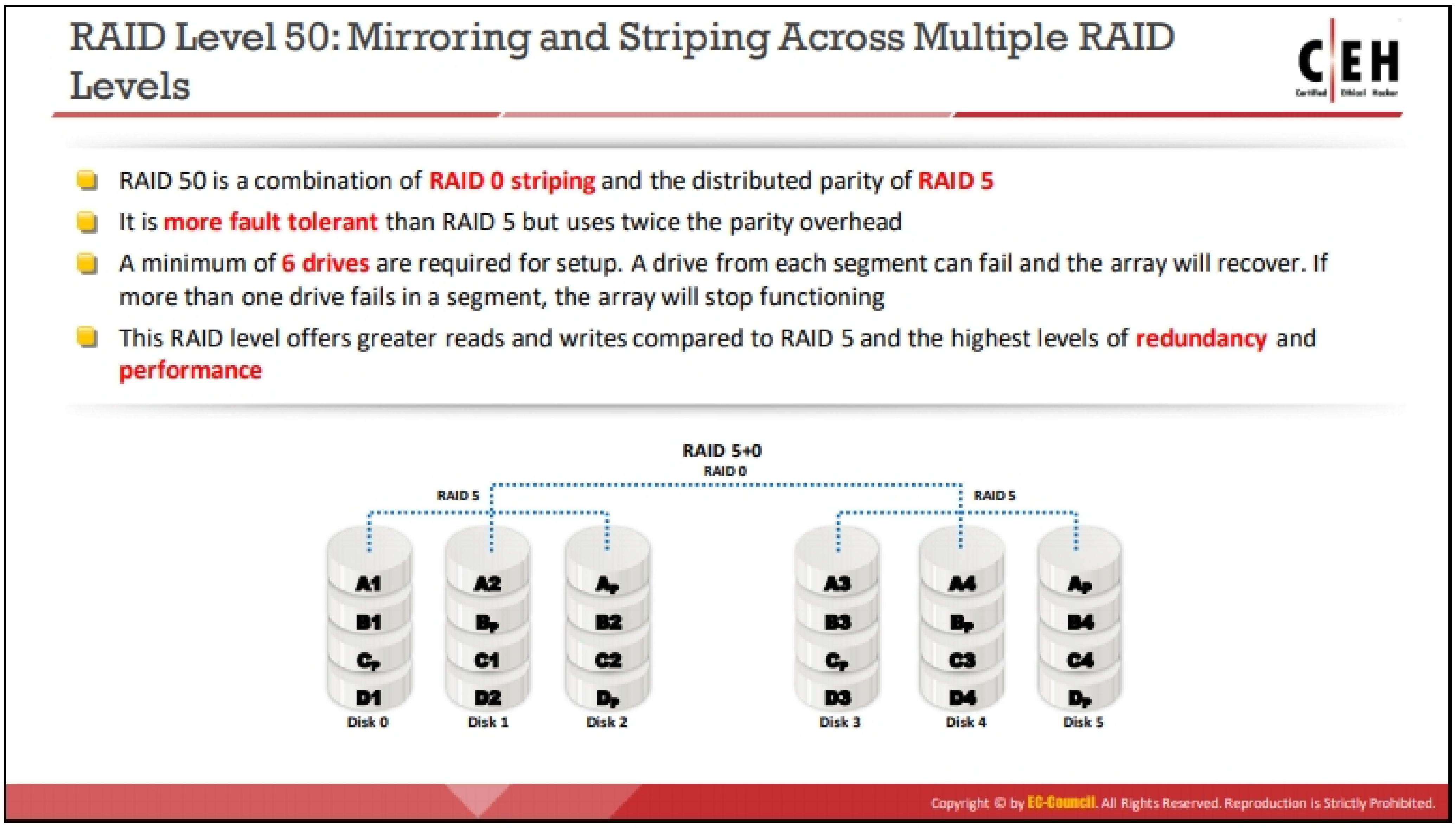
____

____

____

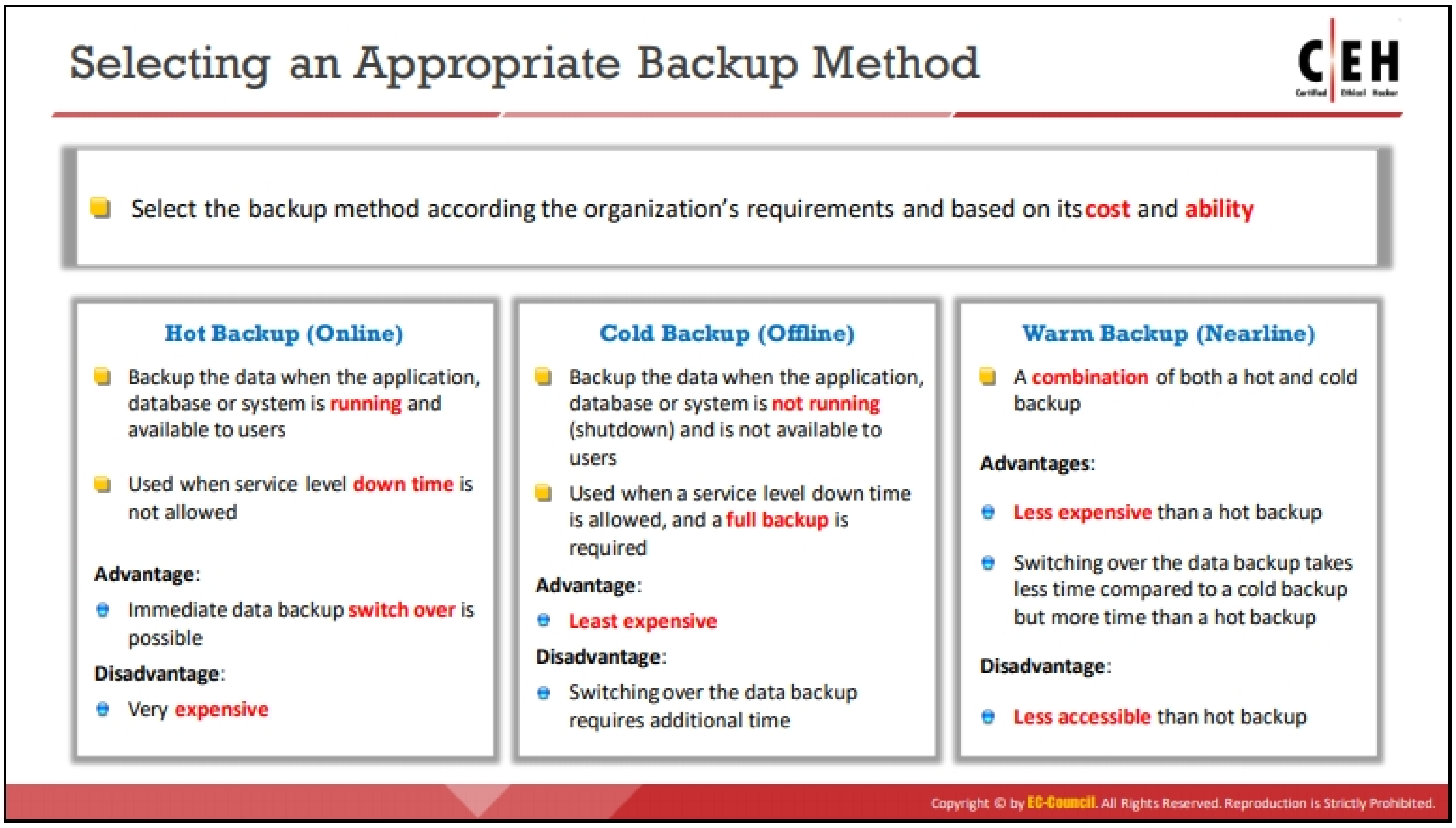
____

____



RAID Level 50: Mirroring and Striping Across Multiple RAID Levels

- RAID 50 is a combination of **RAID 0 striping** and the distributed parity of **RAID 5**
- It is **more fault tolerant** than RAID 5 but uses twice the parity overhead
- A minimum of **6 drives** are required for setup. A drive from each segment can fail and the array will recover. If more than one drive fails in a segment, the array will stop functioning
- This RAID level offers greater reads and writes compared to RAID 5 and the highest levels of **redundancy** and **performance**



Selecting an Appropriate Backup Method

- Select the backup method according the organization's requirements and based on its **cost** and **ability**

Hot Backup (Online)

- Backup the data when the application, database or system is **running** and available to users
- Used when service level **down time** is not allowed

Advantage:

- Immediate data backup **switch over** is possible

Disadvantage:

- Very **expensive**

Cold Backup (Offline)

- Backup the data when the application, database or system is **not running** (shutdown) and is not available to users
- Used when a service level down time is allowed, and a **full backup** is required

Advantage:

- **Least expensive**

Disadvantage:

- Switching over the data backup requires additional time

Warm Backup (Nearline)

- A **combination** of both a hot and cold backup

Advantages:

- **Less expensive** than a hot backup
- Switching over the data backup takes less time compared to a cold backup but more time than a hot backup

Disadvantage:

- **Less accessible** than hot backup

Notes: ____

____

____

____

____

____

Choosing the Backup Location

Onsite Data Backup

- Only storing backup data at **onsite data** storage

Advantages:

- Onsite backup data can be easily accessed and **restored**
- **Less expensive**

Disadvantage:

- Risk of data loss risk is greater

Offsite Data Backup

- Storing backup data in **remote locations** in fire-proof, indestructible safes

Advantage:

- Data is secured from **physical security** threats such as fire or floods

Disadvantage:

- Problems with a regular **data backup schedule**

Cloud Data Backup

- Storing backup data on storage provided by an **online backup** provider

Advantages:

- The data is **encrypted** and free from physical security threats
- Data can be freely **accessed**

Disadvantages:

- **No direct control** of the backup data
- **More time needed** for backup

Data Recovery

- Data recovery is a process for the recovery of data that may have been accidentally or intentionally **deleted** or **corrupted**
- Deleted items include files, folders, and partitions from electronic storage media (hard drives, removable media, optical devices, and other storage media)
- The majority of lost data is **recoverable**. However, there are situations where the damage to the data is permanent and irreversible
- When attempting to recover data from a target, use a variety of data recovery tools

Notes: ____

____

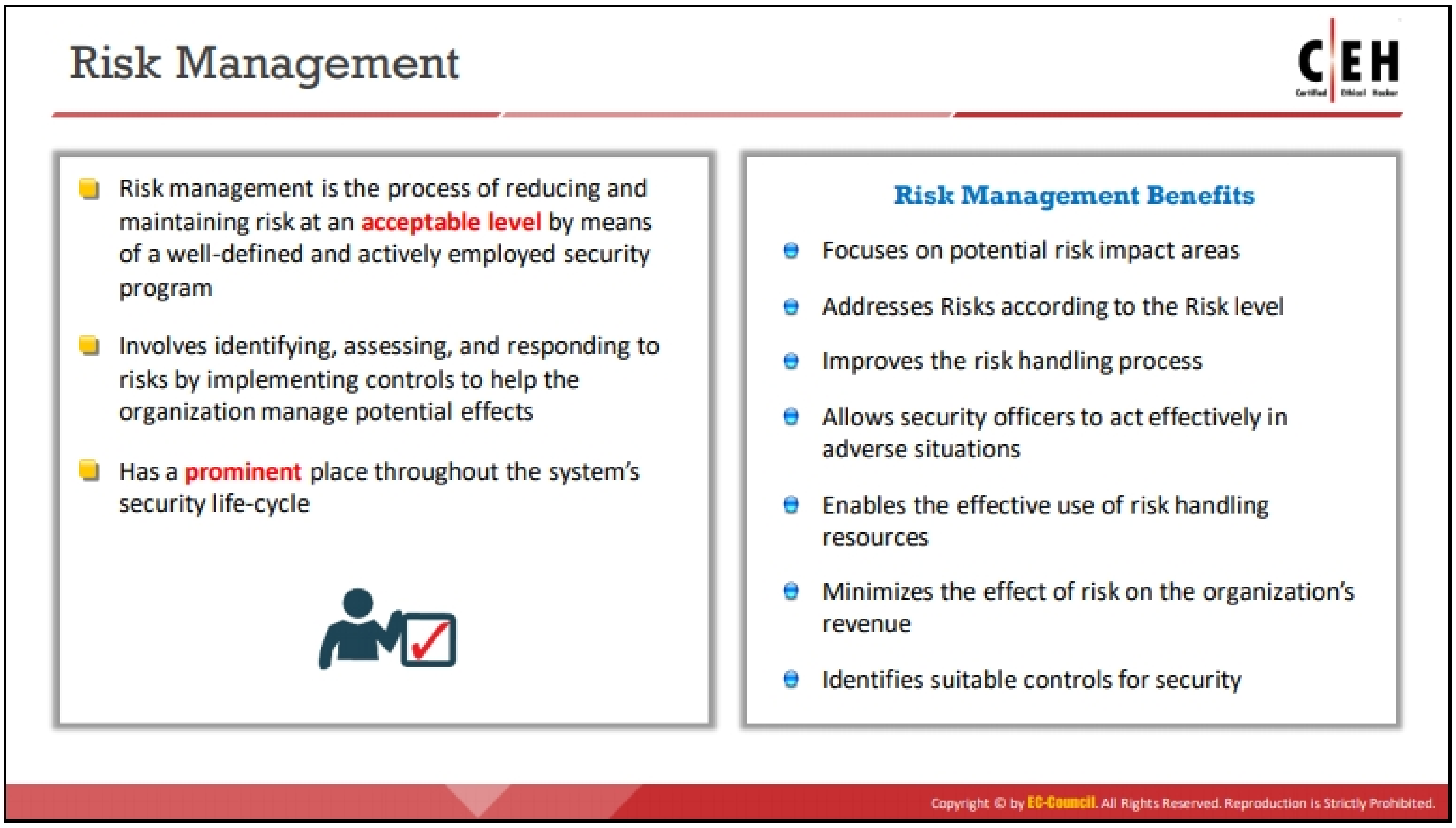
____

____

____

____

Risk Management Concepts



Risk Management

- Risk management is the process of reducing and maintaining risk at an **acceptable level** by means of a well-defined and actively employed security program
- Involves identifying, assessing, and responding to risks by implementing controls to help the organization manage potential effects
- Has a **prominent** place throughout the system's security life-cycle

Risk Management Benefits

- Focuses on potential risk impact areas
- Addresses Risks according to the Risk level
- Improves the risk handling process
- Allows security officers to act effectively in adverse situations
- Enables the effective use of risk handling resources
- Minimizes the effect of risk on the organization's revenue
- Identifies suitable controls for security

Notes: ____

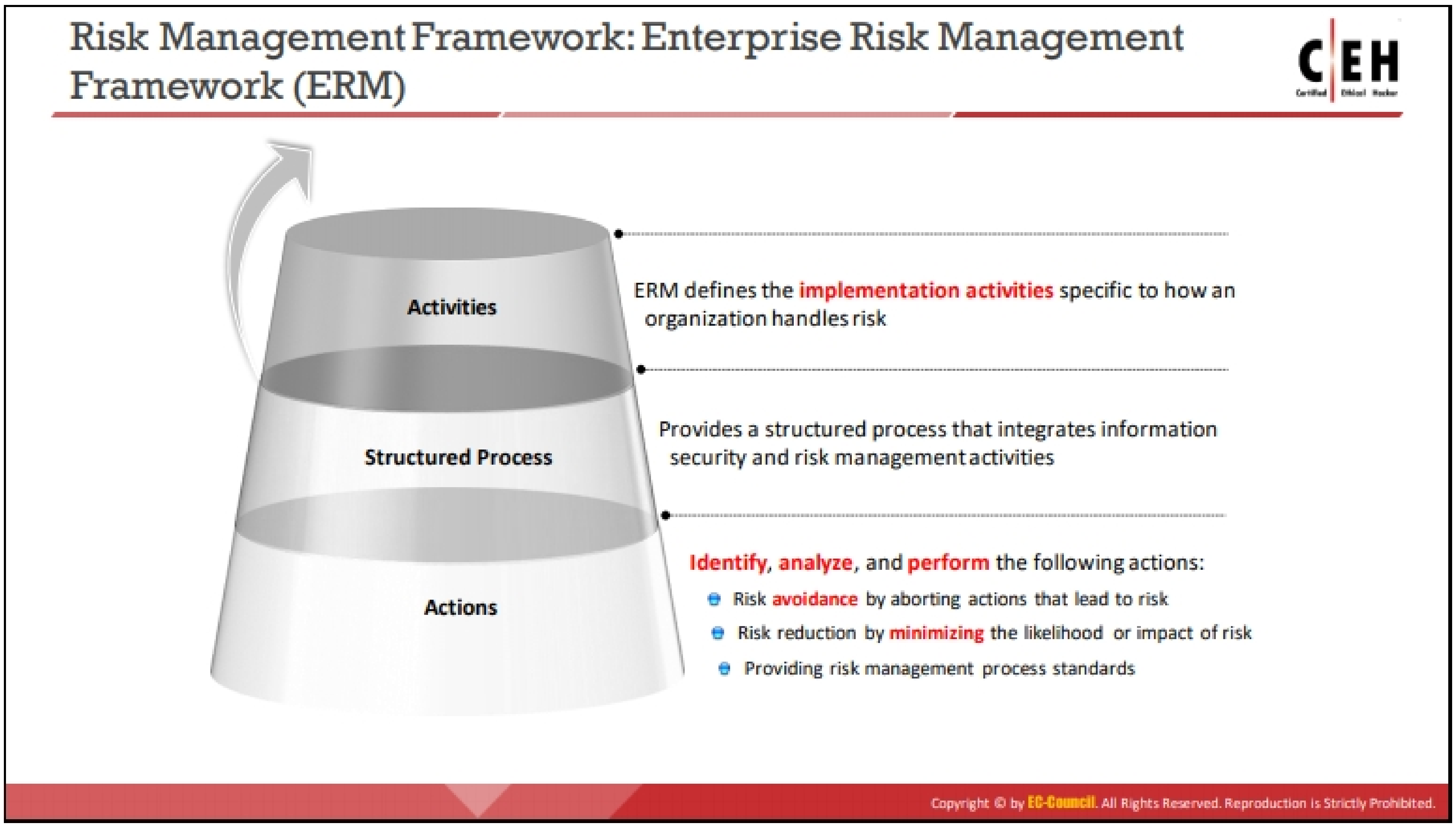
____

____

____

____

____



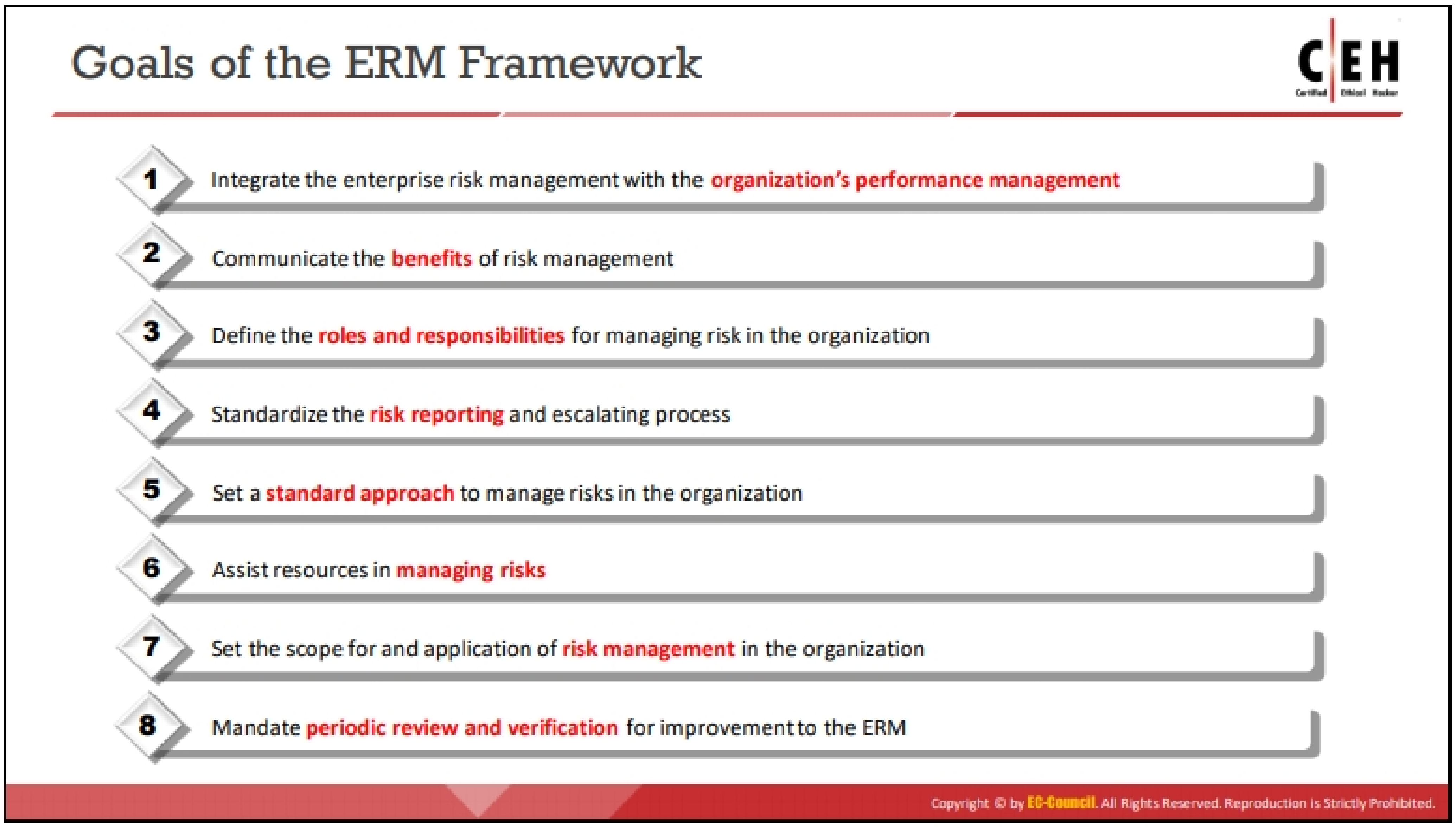
Risk Management Framework: Enterprise Risk Management Framework (ERM)

ERM defines the **implementation activities** specific to how an organization handles risk

Provides a structured process that integrates information security and risk management activities

Identify, **analyze**, and **perform** the following actions:

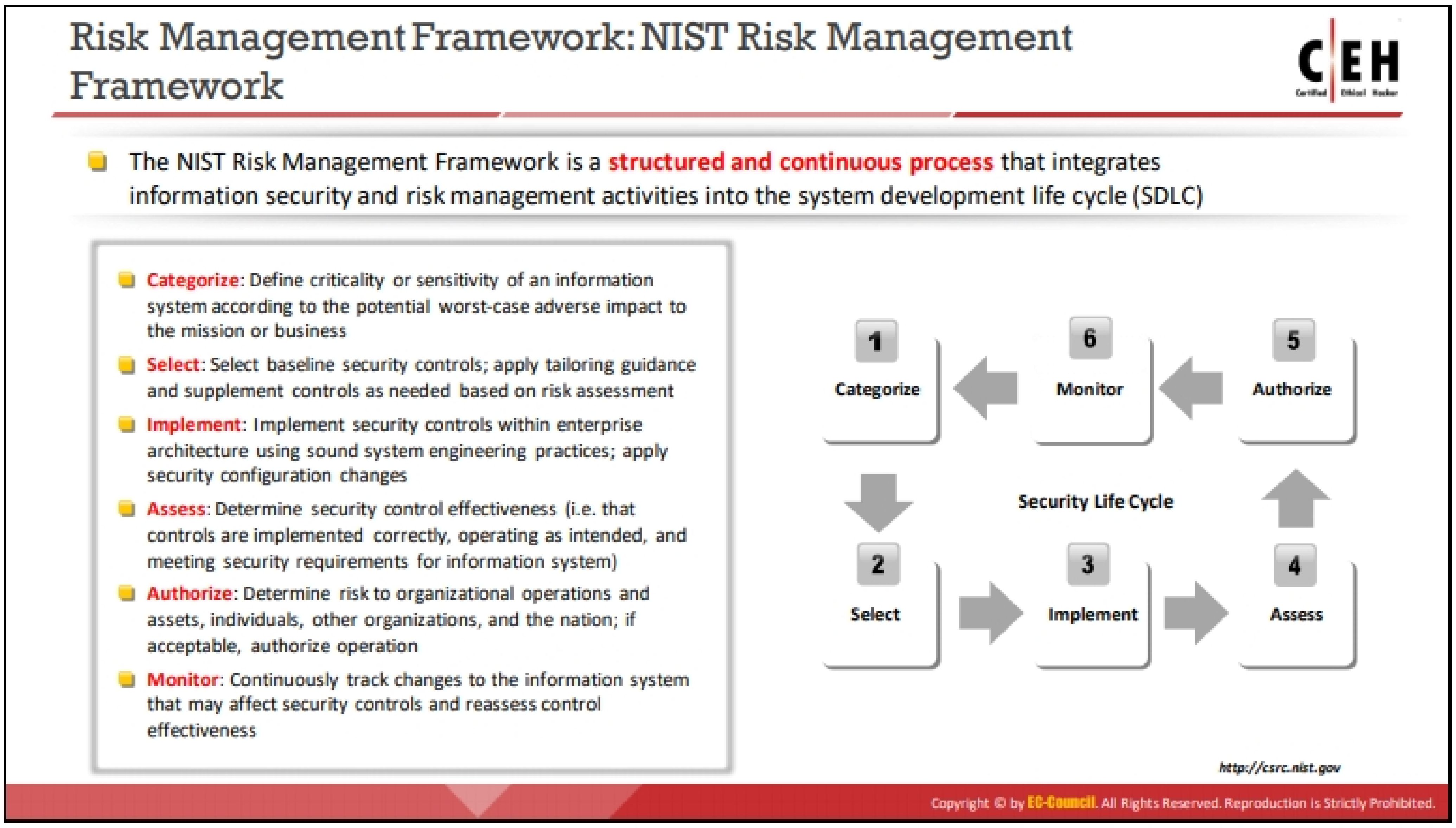
- Risk **avoidance** by aborting actions that lead to risk
- Risk reduction by **minimizing** the likelihood or impact of risk
- Providing risk management process standards



Goals of the ERM Framework

1. Integrate the enterprise risk management with the **organization's performance management**
2. Communicate the **benefits** of risk management
3. Define the **roles and responsibilities** for managing risk in the organization
4. Standardize the **risk reporting** and escalating process
5. Set a **standard approach** to manage risks in the organization
6. Assist resources in **managing risks**
7. Set the scope for and application of **risk management** in the organization
8. Mandate **periodic review and verification** for improvement to the ERM

Notes: ____



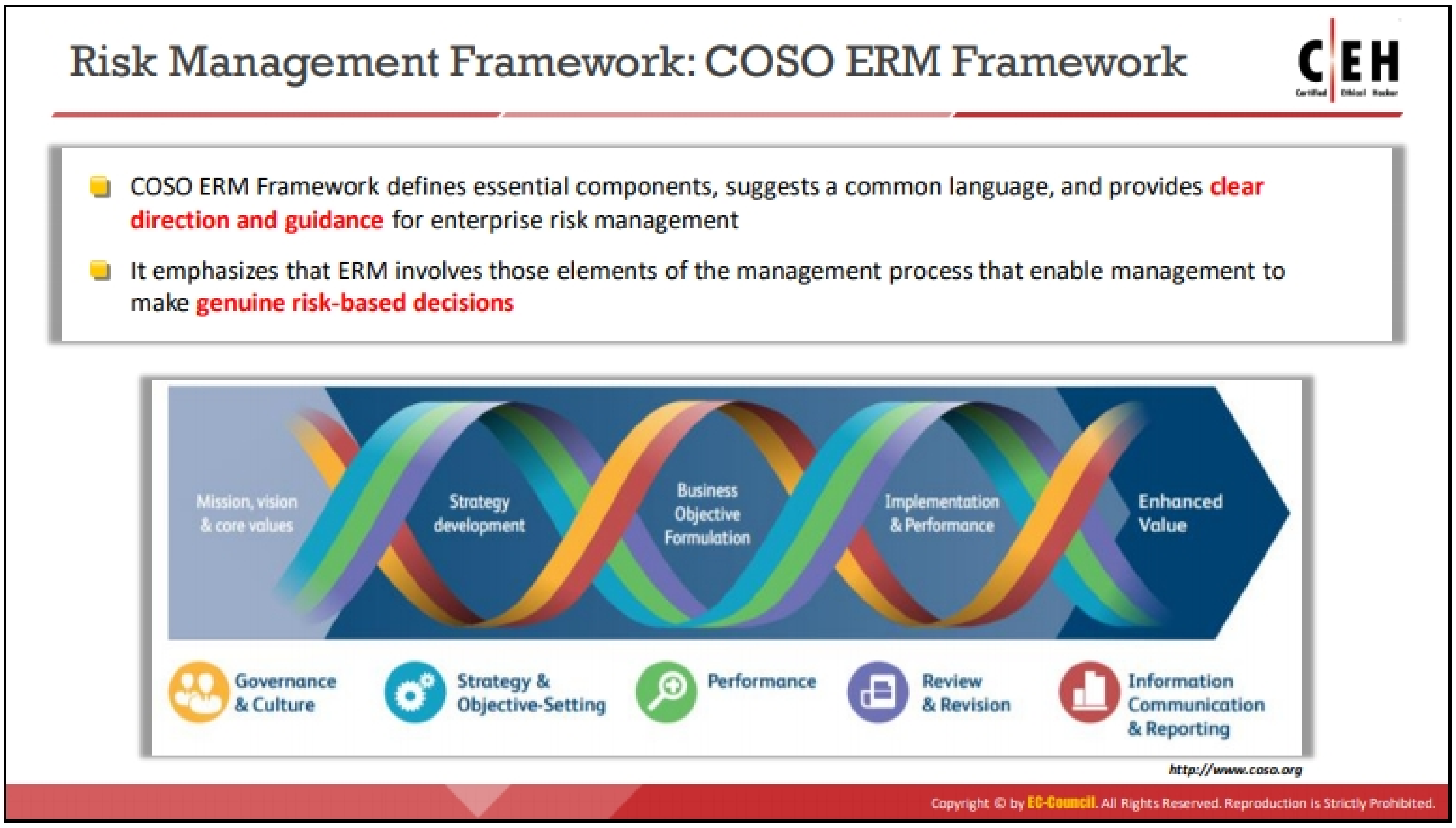
Risk Management Framework: NIST Risk Management Framework

- The NIST Risk Management Framework is a **structured and continuous process** that integrates information security and risk management activities into the system development life cycle (SDLC)

- **Categorize**: Define criticality or sensitivity of an information system according to the potential worst-case adverse impact to the mission or business
- **Select**: Select baseline security controls; apply tailoring guidance and supplement controls as needed based on risk assessment
- **Implement**: Implement security controls within enterprise architecture using sound system engineering practices; apply security configuration changes
- **Assess**: Determine security control effectiveness (i.e. that controls are implemented correctly, operating as intended, and meeting security requirements for information system)
- **Authorize**: Determine risk to organizational operations and assets, individuals, other organizations, and the nation; if acceptable, authorize operation
- **Monitor**: Continuously track changes to the information system that may affect security controls and reassess control effectiveness

1 Categorize
6 Monitor
5 Authorize
Security Life Cycle
2 Select
3 Implement
4 Assess

http://csrc.nist.gov



Risk Management Framework: COSO ERM Framework

- COSO ERM Framework defines essential components, suggests a common language, and provides **clear direction and guidance** for enterprise risk management
- It emphasizes that ERM involves those elements of the management process that enable management to make **genuine risk-based decisions**

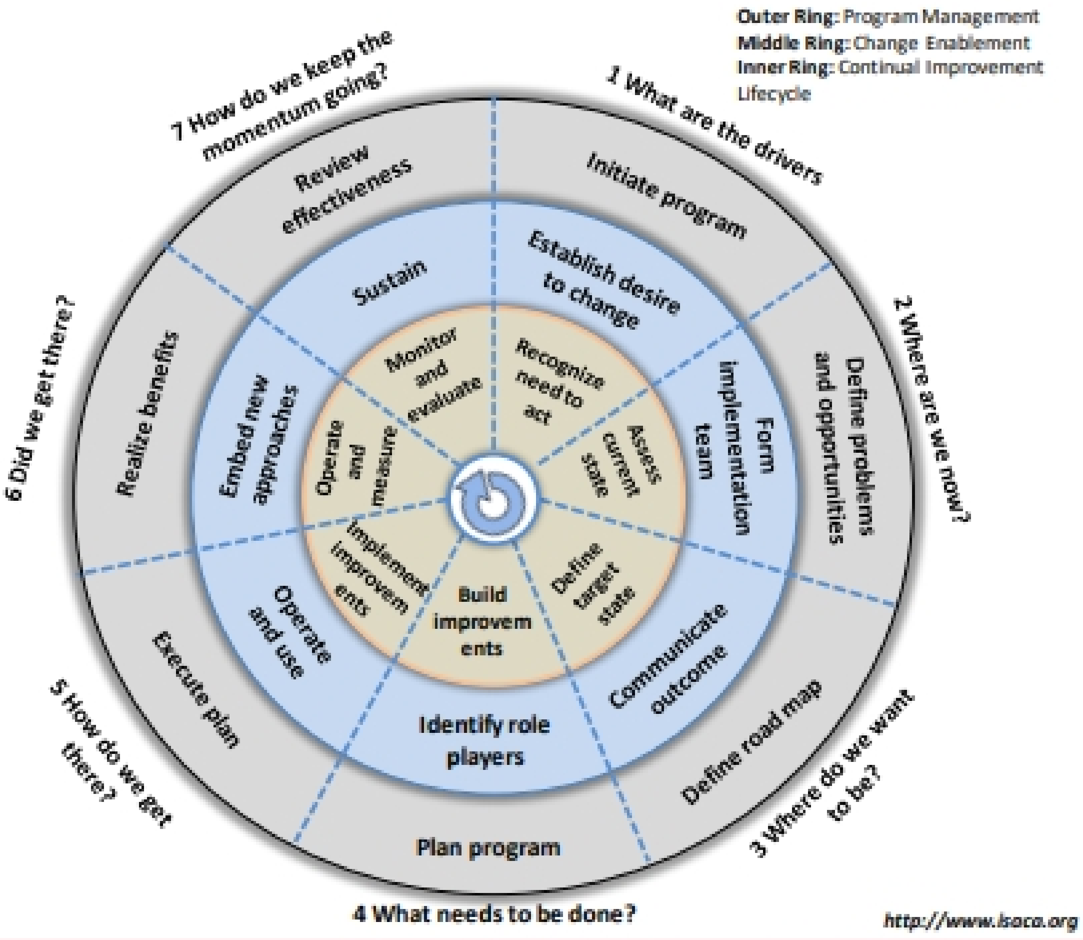
Mission, vision & core values
Strategy development
Business Objective Formulation
Implementation & Performance
Enhanced Value
Governance & Culture
Strategy & Objective-Setting
Performance
Review & Revision
Information Communication & Reporting

http://www.coso.org

Notes:

Risk Management Framework: COBIT Framework

- COBIT Framework is an IT governance framework and supporting toolset that allows managers to bridge the gap between control requirements, technical issues, and business risks
- It emphasizes regulatory compliance, helps organizations to increase the value attained from IT, and enables alignment and simplifies implementation of the enterprise's IT governance and control framework


Outer Ring: Program Management
Middle Ring: Change Enablement
Inner Ring: Continual Improvement Lifecycle
1 What are the drivers
2 Where are we now?
3 Where do we want to be?
4 What needs to be done?
5 How do we get there?
6 Did we get there?
7 How do we keep the momentum going?
Initiate program
Define problems and opportunities
Define road map
Plan program
Execute plan
Realize benefits
Review effectiveness
Establish desire to change
Form implementation team
Communicate outcome
Identify role players
Operate and use
Embed new approaches
Sustain
Recognize need to act
Assess current state
Define target state
Build improvements
Implement improvements
Operate and measure
Monitor and evaluate

http://www.isaca.org

Enterprise Network Risk Management Policy

- Risk Management Policy assists in developing and establishing essential processes and procedures to address and minimize information security risks
- It outlines different aspects of risk and identifies people to manage the risk in the organization

Objectives:

- Equip the organization with the required skills to identify and treat risks
- Provide a consistent risk management framework
- Provide the overall direction and purpose for performing risk management
- Manage the risks with adequate risk mitigation techniques
- Combat the existing and emerging risks
- Integrate operational risks into the risk management process
- Accomplish the strategic and operational goals of the organization
- Facilitate assistance in taking strategic management decisions
- Meet legal and regulatory requirements

Notes: ____

Risk Mitigation

- Risk mitigation includes all possible solutions for reducing the **probability of risk** and limiting the impact of a risk if it occurs
- It should identify the mitigation strategies for the risks that fall outside the department's **risk tolerance** and provide an understanding of the level of risk with controls and treatments
- It identifies the priority order in which individual risks should be **mitigated**, **monitored**, and **reviewed**

Risk Mitigation Strategies

1. **Risk Assumption**
2. **Risk Avoidance**
3. **Risk Limitation**
4. **Risk Planning**
5. **Research and Acknowledgment**
6. **Risk Transference**

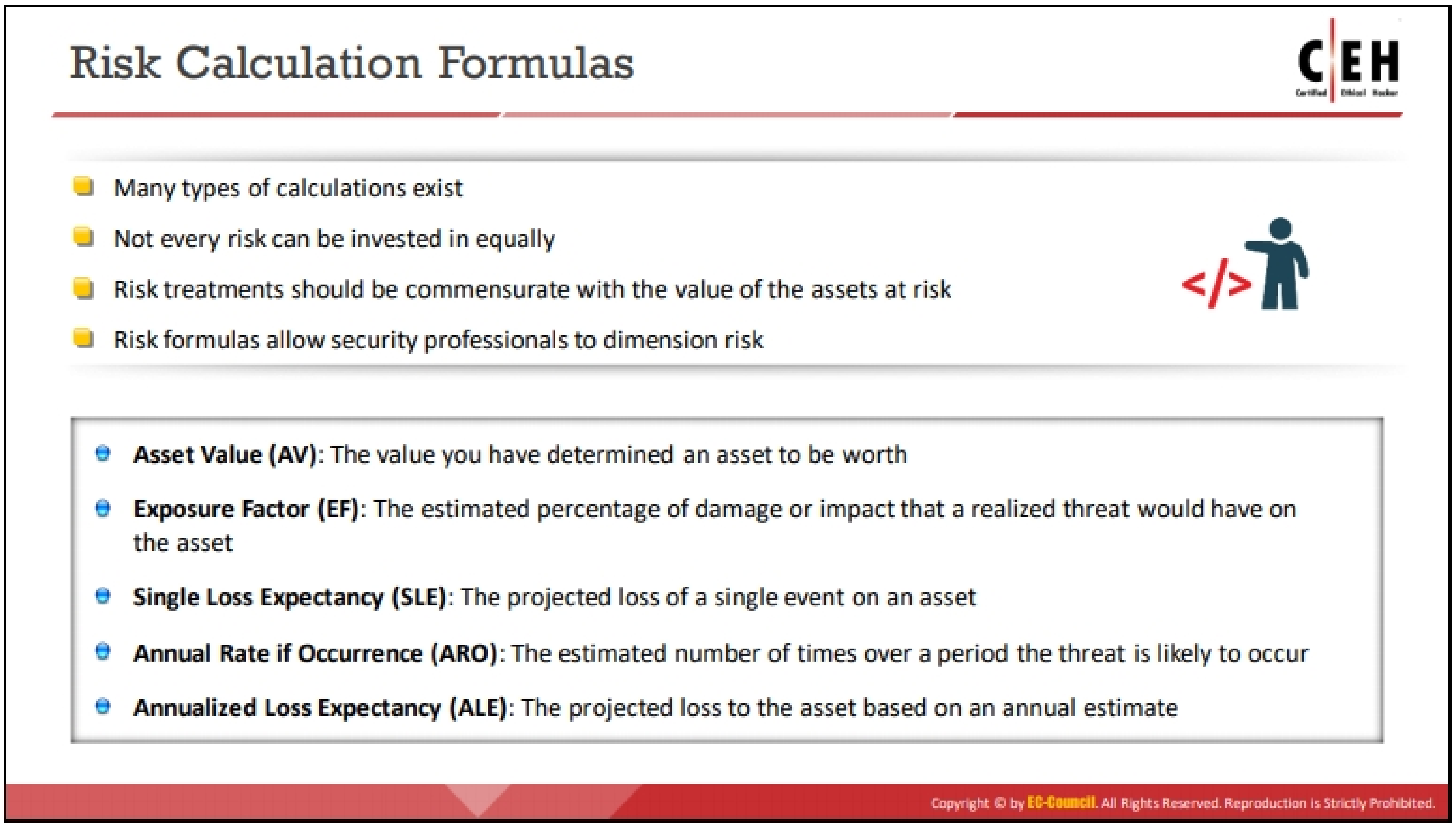
Control the Risks

- Identify all existing security controls that can help organizations in **reducing security risks**
- Recommend any new security controls the organization must implement
- Use the results of vulnerability and threat assessment to minimize risks, as risks are directly proportionate to them

Some of the security controls that help in reducing risks include:

1. Impart **security awareness** to employees
2. Place up-to-date hardware and software **security solutions** such as IDS, firewall, honeypot, and DMZ
3. Strengthen network, account, application, device, and **physical security** across the organization
4. Implement **strict access controls** and security policies
5. Deploy **encryption** for all data transfers
6. Implement an **appropriate incident handling** and response plan

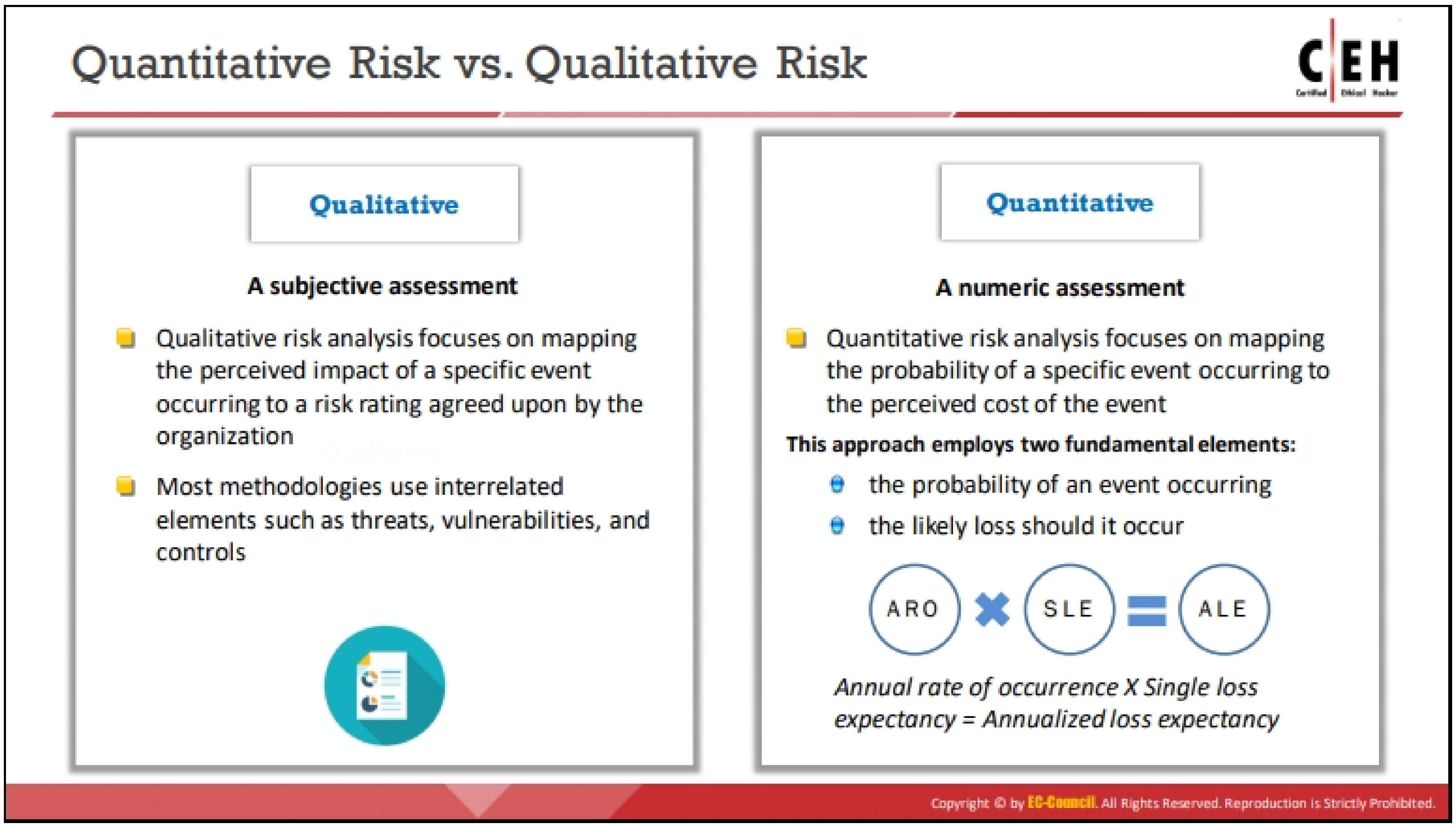
Notes: ____



Risk Calculation Formulas

- Many types of calculations exist
- Not every risk can be invested in equally
- Risk treatments should be commensurate with the value of the assets at risk
- Risk formulas allow security professionals to dimension risk

- **Asset Value (AV)**: The value you have determined an asset to be worth
- **Exposure Factor (EF)**: The estimated percentage of damage or impact that a realized threat would have on the asset
- **Single Loss Expectancy (SLE)**: The projected loss of a single event on an asset
- **Annual Rate if Occurrence (ARO)**: The estimated number of times over a period the threat is likely to occur
- **Annualized Loss Expectancy (ALE)**: The projected loss to the asset based on an annual estimate



Quantitative Risk vs. Qualitative Risk

Qualitative

A subjective assessment

- Qualitative risk analysis focuses on mapping the perceived impact of a specific event occurring to a risk rating agreed upon by the organization
- Most methodologies use interrelated elements such as threats, vulnerabilities, and controls

Quantitative

A numeric assessment

- Quantitative risk analysis focuses on mapping the probability of a specific event occurring to the perceived cost of the event

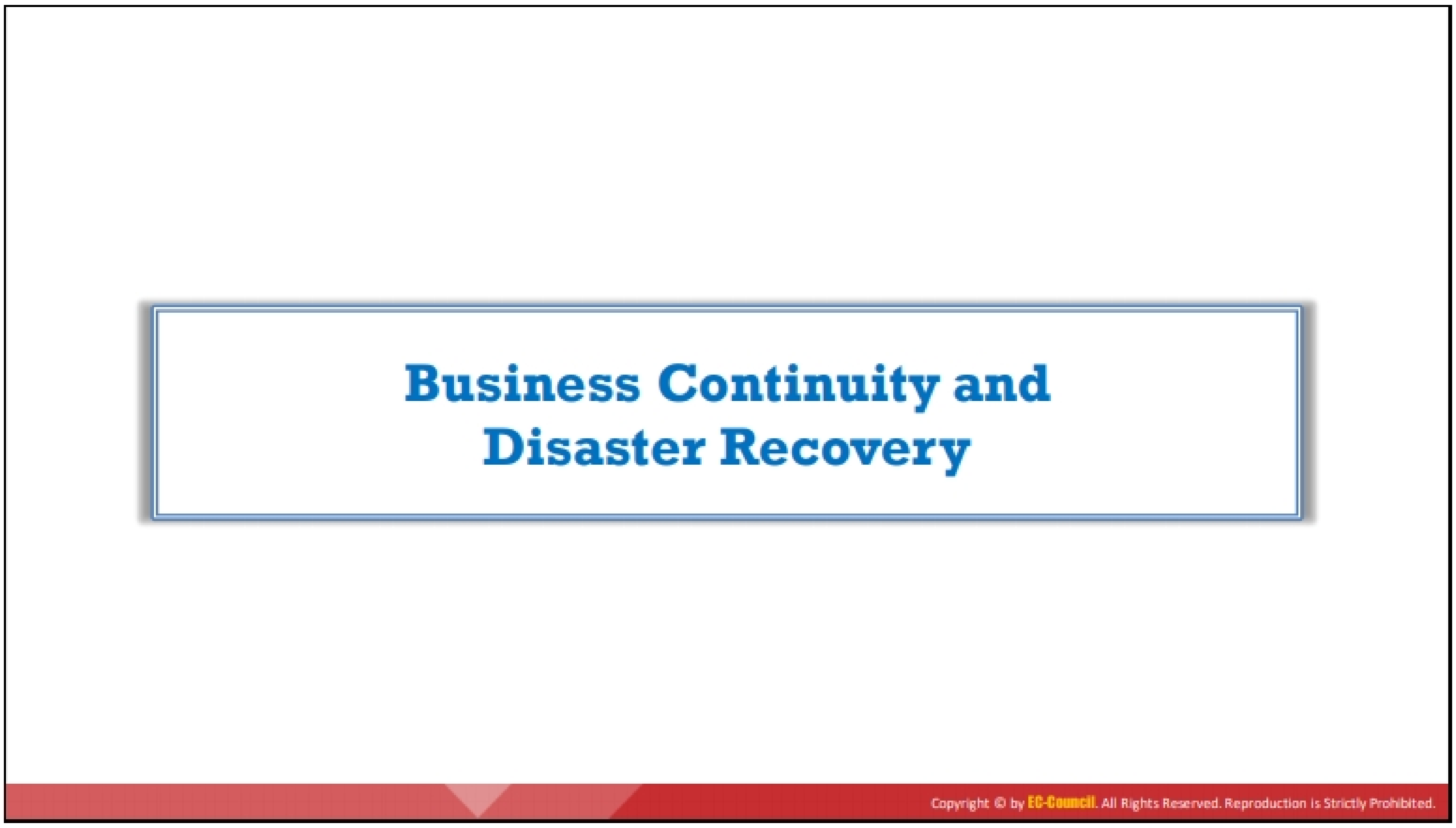
This approach employs two fundamental elements:

- the probability of an event occurring
- the likely loss should it occur

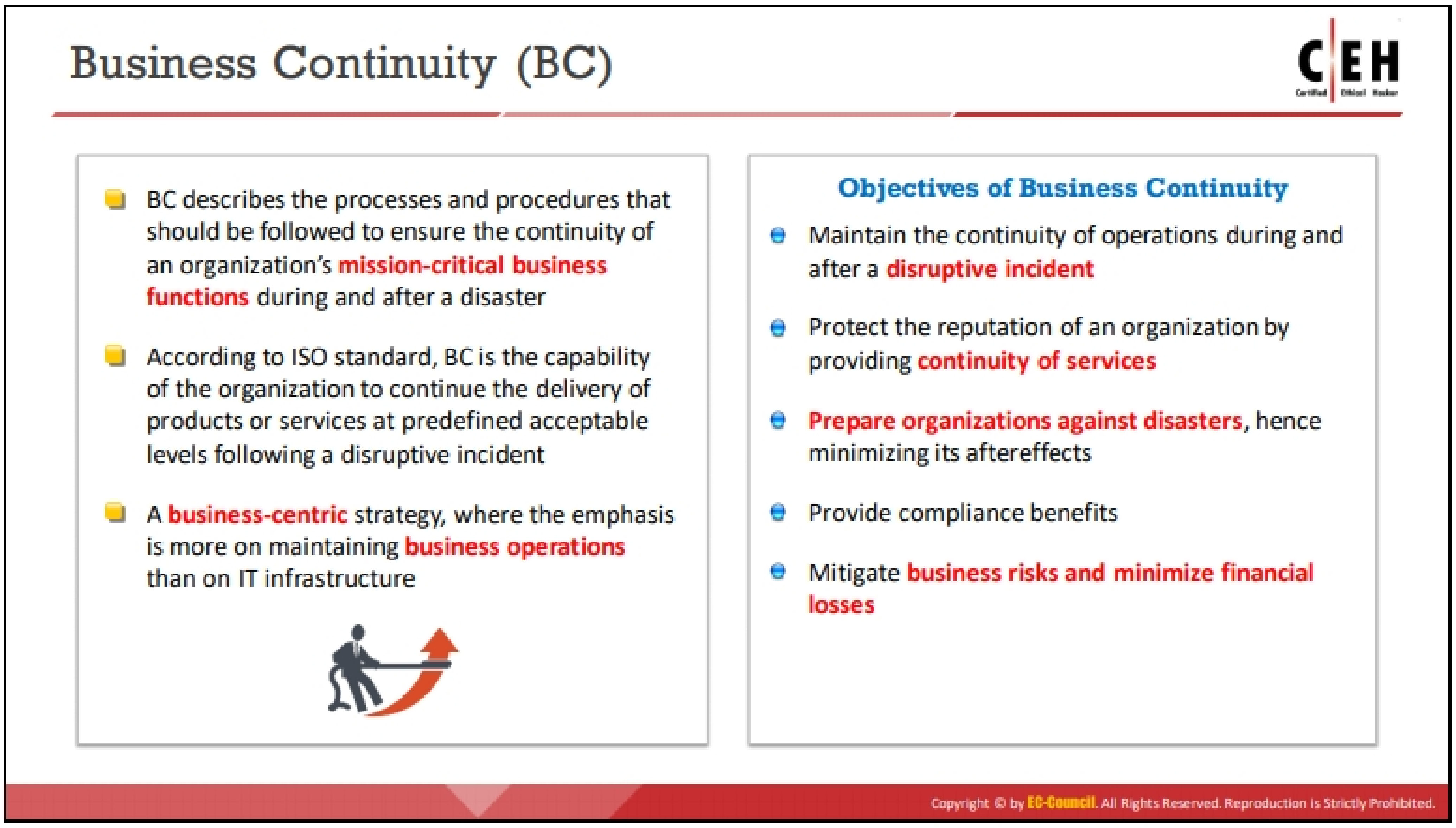
ARO ✖ SLE = ALE

Annual rate of occurrence X Single loss expectancy = Annualized loss expectancy

Notes: ______



Business Continuity and Disaster Recovery



Business Continuity (BC)

- BC describes the processes and procedures that should be followed to ensure the continuity of an organization's **mission-critical business functions** during and after a disaster
- According to ISO standard, BC is the capability of the organization to continue the delivery of products or services at predefined acceptable levels following a disruptive incident
- A **business-centric** strategy, where the emphasis is more on maintaining **business operations** than on IT infrastructure

Objectives of Business Continuity

- Maintain the continuity of operations during and after a **disruptive incident**
- Protect the reputation of an organization by providing **continuity of services**
- **Prepare organizations against disasters**, hence minimizing its aftereffects
- Provide compliance benefits
- Mitigate **business risks and minimize financial losses**

Notes: ____

____

____

____

____

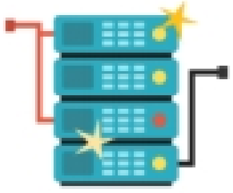
____

Disaster Recovery (DR)

- DR refers to the organization’s ability to **restore their business data and applications**, even after a disaster
- Includes the recovery of the systems and people responsible for rebuilding the data centers, servers, or other infrastructure damaged in a disruptive incident
- A **data-centric strategy** that emphasizes quickly restoring an organization’s IT infrastructure and data

Objectives of Disaster Recovery

- Reduce the downtime faced by an organization during and after a disruptive incident
- Reduce the accrual of losses during and after a disaster
- Recover any data that are damaged due to a hardware failure



Business Impact Analysis (BIA)

1 BIA is a systematic process that **determines and evaluates the potential effects** of an interruption to critical business operations as a result of a disaster, accident, or emergency

2 It ascertains the recovery time and recovery requirements for various disaster scenarios

3 The underlying assumption in a BIA is that while each component of an organization is reliant upon the **continued functioning** of every other component, some are more crucial than others, and limited funds should be **prioritized** to ensure recovery in the **wake of a disaster**

4 An analysis tool; it does not **focus** on the design or implementation of **recovery solutions**

Notes: ____

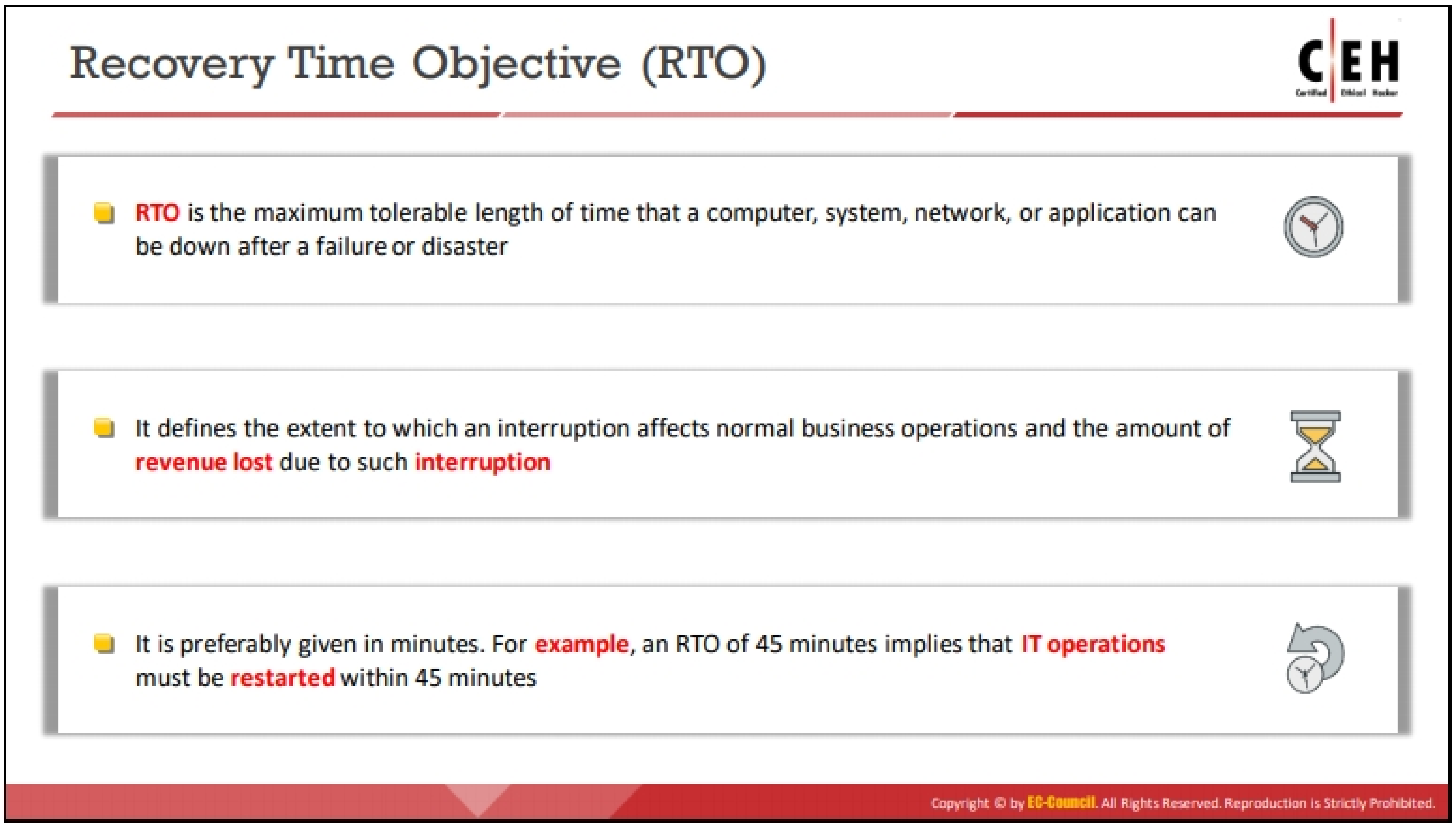
____

____

____

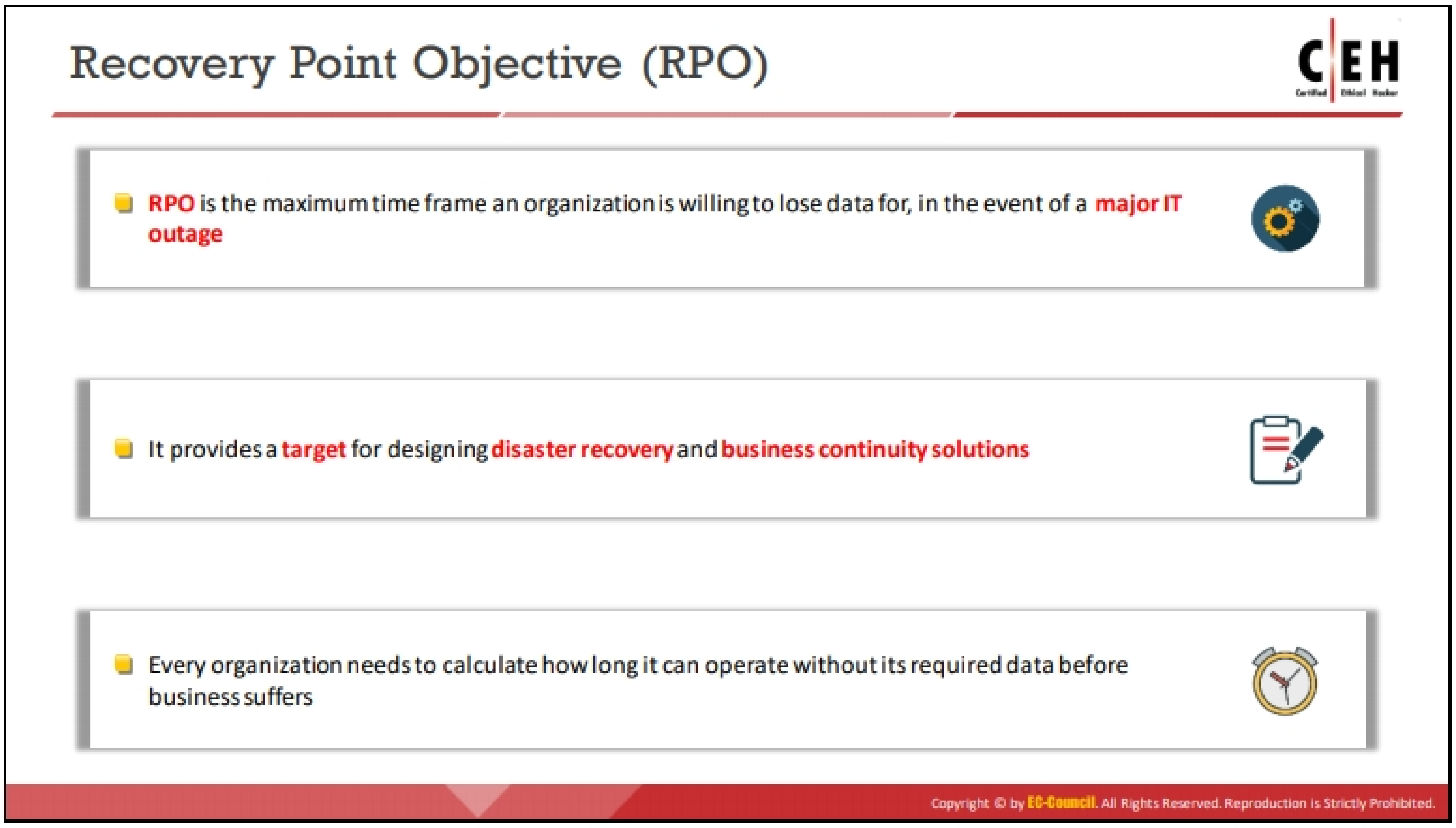
____

____



Recovery Time Objective (RTO)

- **RTO** is the maximum tolerable length of time that a computer, system, network, or application can be down after a failure or disaster
- It defines the extent to which an interruption affects normal business operations and the amount of **revenue lost** due to such **interruption**
- It is preferably given in minutes. For **example**, an RTO of 45 minutes implies that **IT operations** must be **restarted** within 45 minutes



Recovery Point Objective (RPO)

- **RPO** is the maximum time frame an organization is willing to lose data for, in the event of a **major IT outage**
- It provides a **target** for designing **disaster recovery** and **business continuity solutions**
- Every organization needs to calculate how long it can operate without its required data before business suffers

Notes: ____

Business Continuity Plan (BCP)

- A BCP is a comprehensive document that is formulated to **ensure resilience against potential threats** and allow the operations to continue under adverse or abnormal conditions

BCP Goals

- Analyzing the potential risks and losses
- Enabling the risk management process to lessen the prospect of a disruption to the worst-case scenario of shutting down the business completely
- Prioritizing the safety, health, and welfare of the organization and its staff
- Minimizing infrastructural damage in the event of a disaster
- Recuperating to normal operating conditions after a disruption
- Maintaining vital documents and details, such as telephone numbers, employee details, vendor details, and client details
- Providing training and awareness to staff on their roles and responsibilities, to keep them better prepared

Disaster Recovery Plan (DRP)

- A DRP is developed for specific departments within an organization to allow them to **recover from a disaster**

DRP Goals

- Reduce overall organizational risk
- Alleviate senior management concerns
- Ensure compliance with regulations
- Ensure rapid response to incidents

Notes:

Cyber Threat Intelligence

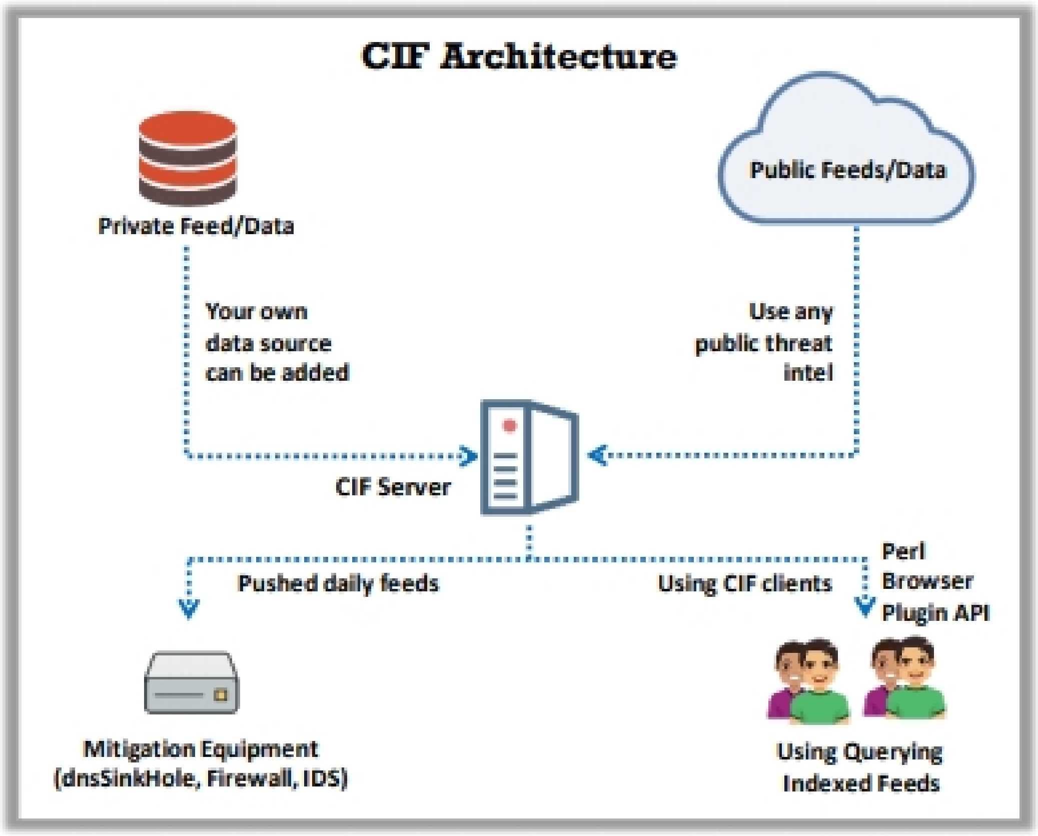
Threat Intelligence Frameworks

Collective Intelligence Framework (CIF)

- Collective Intelligence Framework (CIF) is a cyber threat intelligence management system that allows you to **combine known malicious threat information** from many sources and use that information for incident detection, response, and mitigation

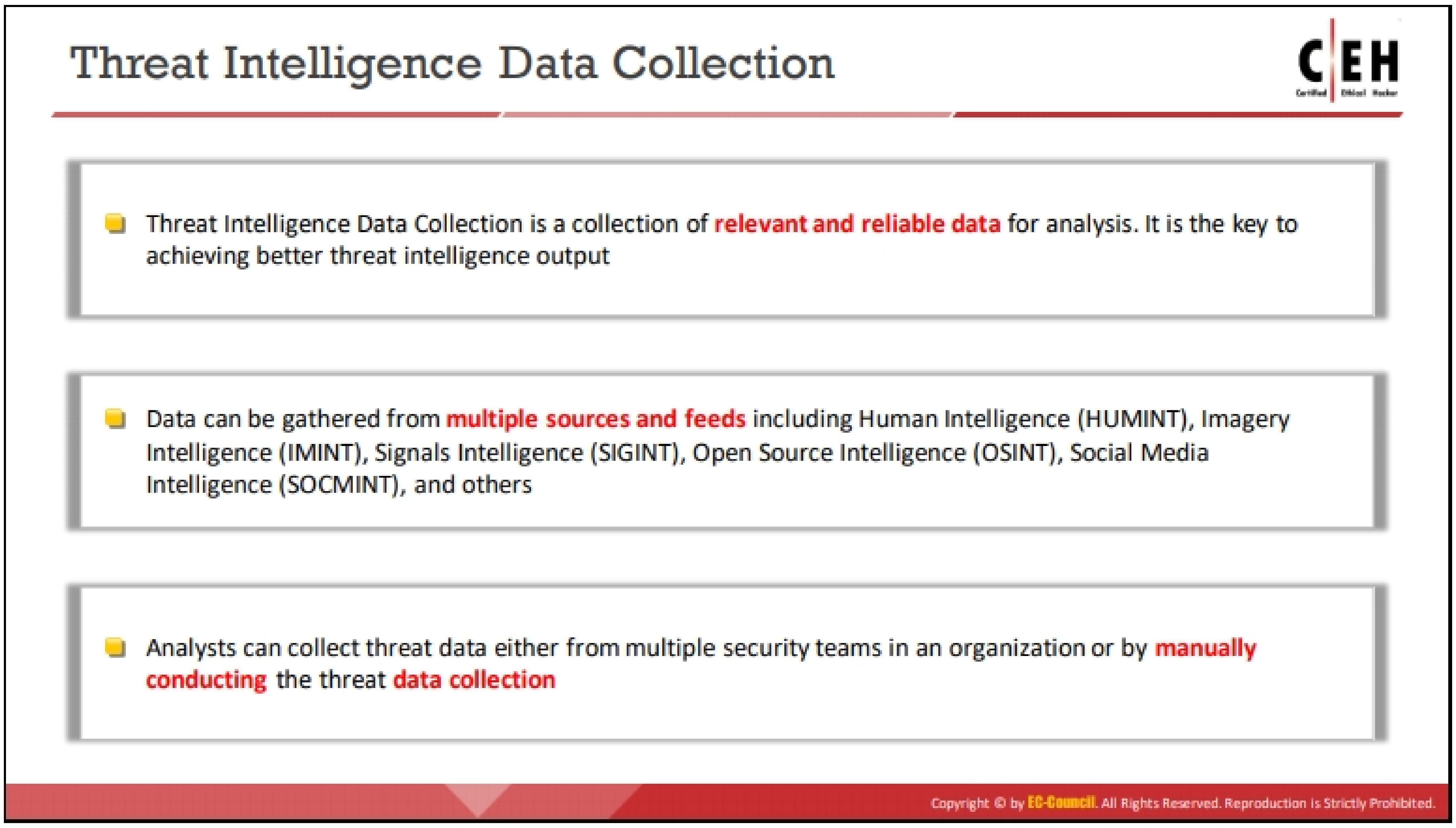
- CIF helps to parse, normalize, store, post-process, query, share, and **produce data sets of threat intelligence**

CIF Architecture


Private Feed/Data
Public Feeds/Data
Your own data source can be added
Use any public threat intel
CIF Server
Pushed daily feeds
Using CIF clients
Perl
Browser
Plugin API
Mitigation Equipment (dnsSinkHole, Firewall, IDS)
Using Querying Indexed Feeds

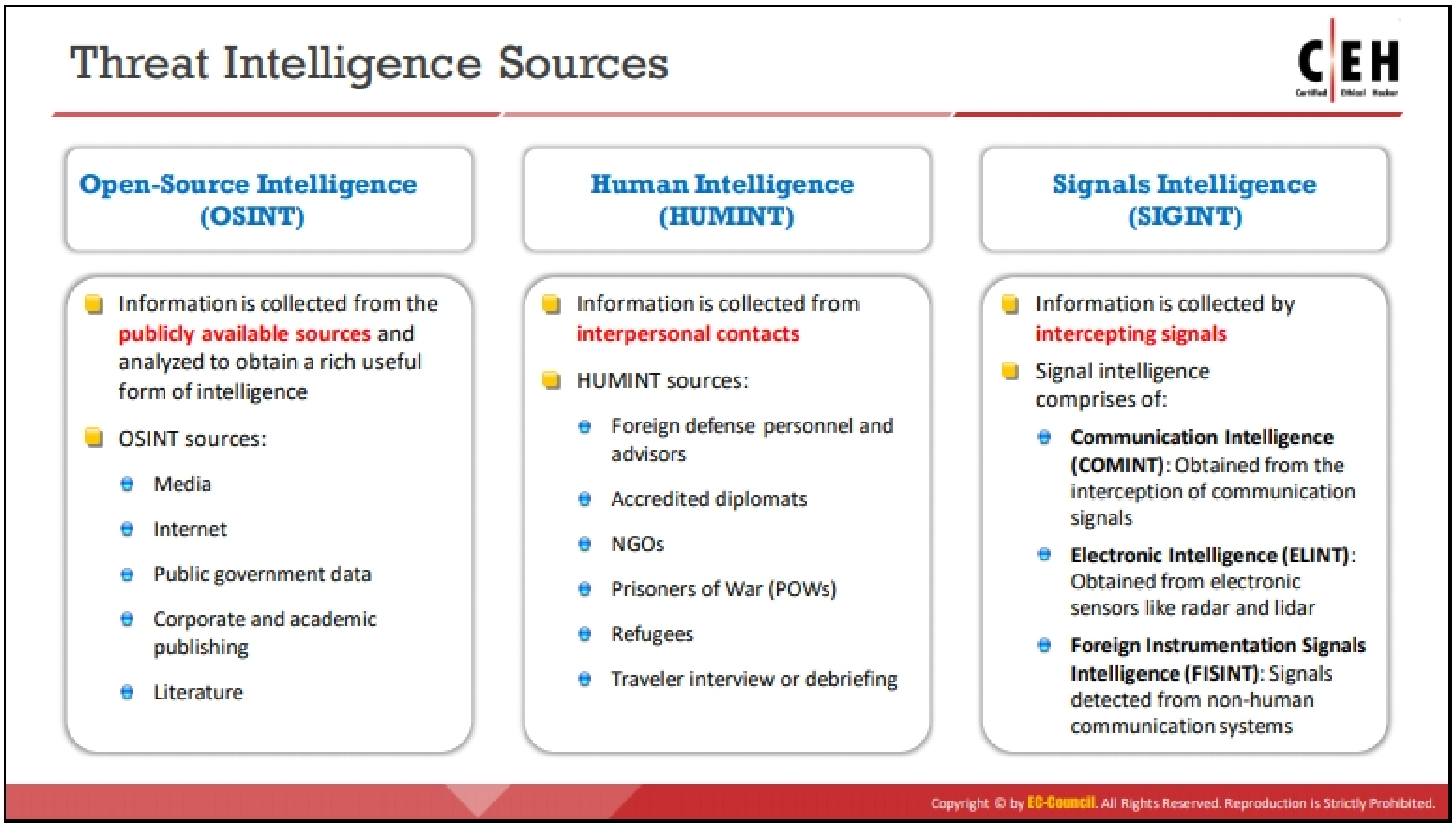
https://csirtgadgets.com

Notes:



Threat Intelligence Data Collection

- Threat Intelligence Data Collection is a collection of **relevant and reliable data** for analysis. It is the key to achieving better threat intelligence output
- Data can be gathered from **multiple sources and feeds** including Human Intelligence (HUMINT), Imagery Intelligence (IMINT), Signals Intelligence (SIGINT), Open Source Intelligence (OSINT), Social Media Intelligence (SOCMINT), and others
- Analysts can collect threat data either from multiple security teams in an organization or by **manually conducting** the threat **data collection**



Threat Intelligence Sources

Open-Source Intelligence (OSINT)

- Information is collected from the **publicly available sources** and analyzed to obtain a rich useful form of intelligence
- OSINT sources:
  - Media
  - Internet
  - Public government data
  - Corporate and academic publishing
  - Literature

Human Intelligence (HUMINT)

- Information is collected from **interpersonal contacts**
- HUMINT sources:
  - Foreign defense personnel and advisors
  - Accredited diplomats
  - NGOs
  - Prisoners of War (POWs)
  - Refugees
  - Traveler interview or debriefing

Signals Intelligence (SIGINT)

- Information is collected by **intercepting signals**
- Signal intelligence comprises of:
  - **Communication Intelligence (COMINT)**: Obtained from the interception of communication signals
  - **Electronic Intelligence (ELINT)**: Obtained from electronic sensors like radar and lidar
  - **Foreign Instrumentation Signals Intelligence (FISINT)**: Signals detected from non-human communication systems

Notes: ____

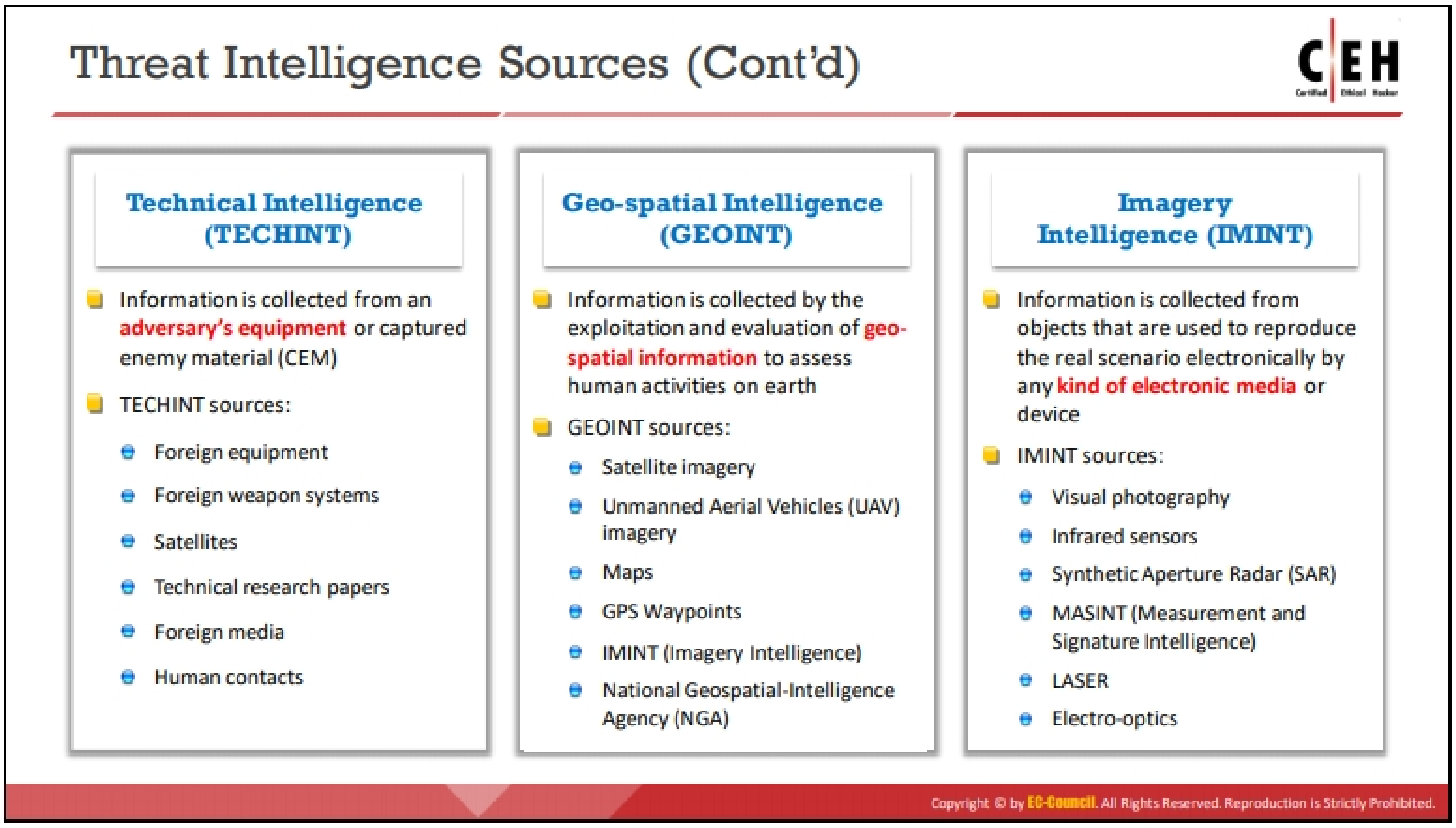
____

____

____

____

____



Threat Intelligence Sources (Cont'd)

Technical Intelligence (TECHINT)

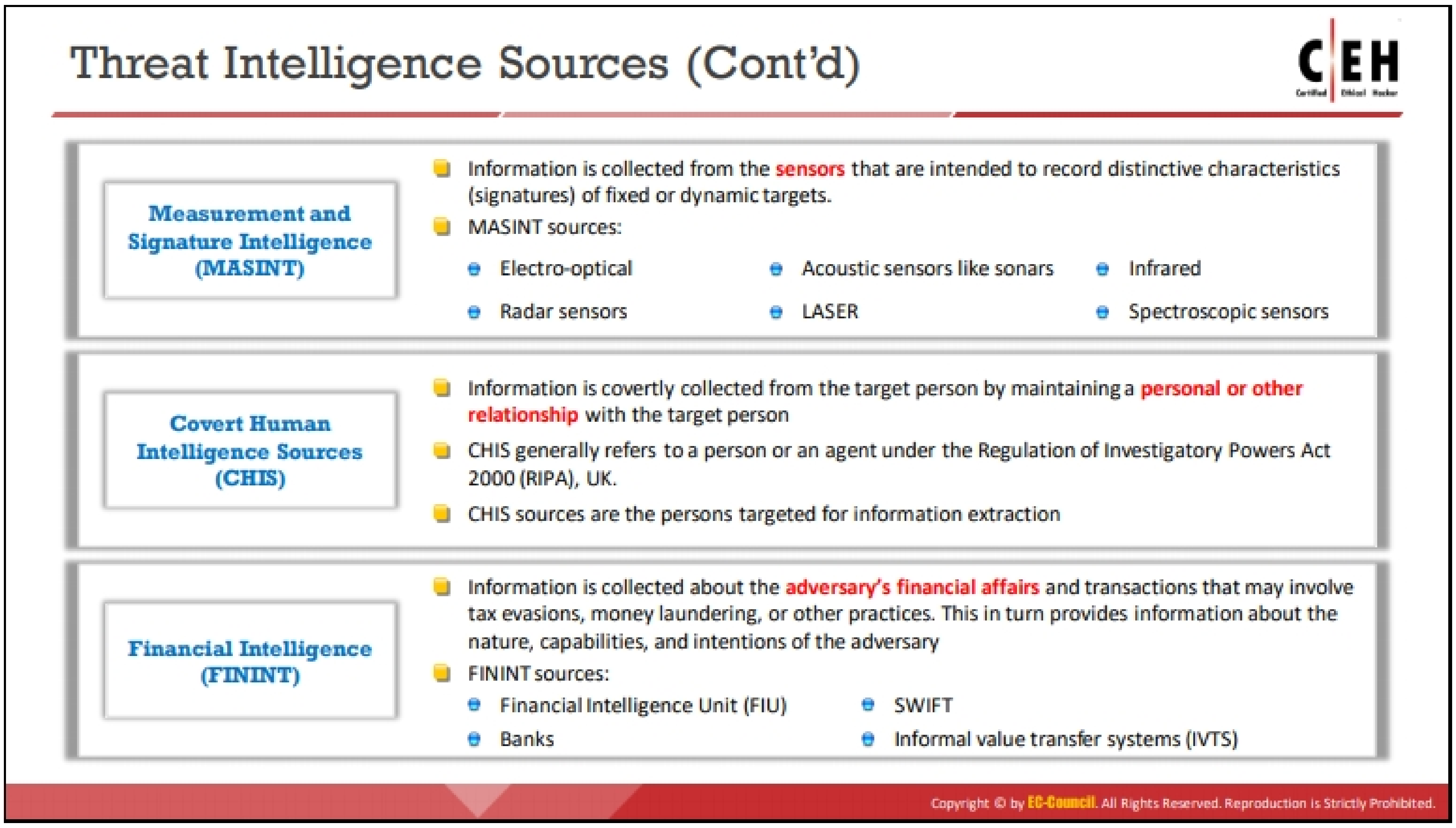
- Information is collected from an **adversary's equipment** or captured enemy material (CEM)
- TECHINT sources:
  - Foreign equipment
  - Foreign weapon systems
  - Satellites
  - Technical research papers
  - Foreign media
  - Human contacts

Geo-spatial Intelligence (GEOINT)

- Information is collected by the exploitation and evaluation of **geo-spatial information** to assess human activities on earth
- GEOINT sources:
  - Satellite imagery
  - Unmanned Aerial Vehicles (UAV) imagery
  - Maps
  - GPS Waypoints
  - IMINT (Imagery Intelligence)
  - National Geospatial-Intelligence Agency (NGA)

Imagery Intelligence (IMINT)

- Information is collected from objects that are used to reproduce the real scenario electronically by any **kind of electronic media** or device
- IMINT sources:
  - Visual photography
  - Infrared sensors
  - Synthetic Aperture Radar (SAR)
  - MASINT (Measurement and Signature Intelligence)
  - LASER
  - Electro-optics



Threat Intelligence Sources (Cont'd)

Measurement and Signature Intelligence (MASINT)

- Information is collected from the **sensors** that are intended to record distinctive characteristics (signatures) of fixed or dynamic targets.
- MASINT sources:
  - Electro-optical
  - Radar sensors
  - Acoustic sensors like sonars
  - LASER
  - Infrared
  - Spectroscopic sensors

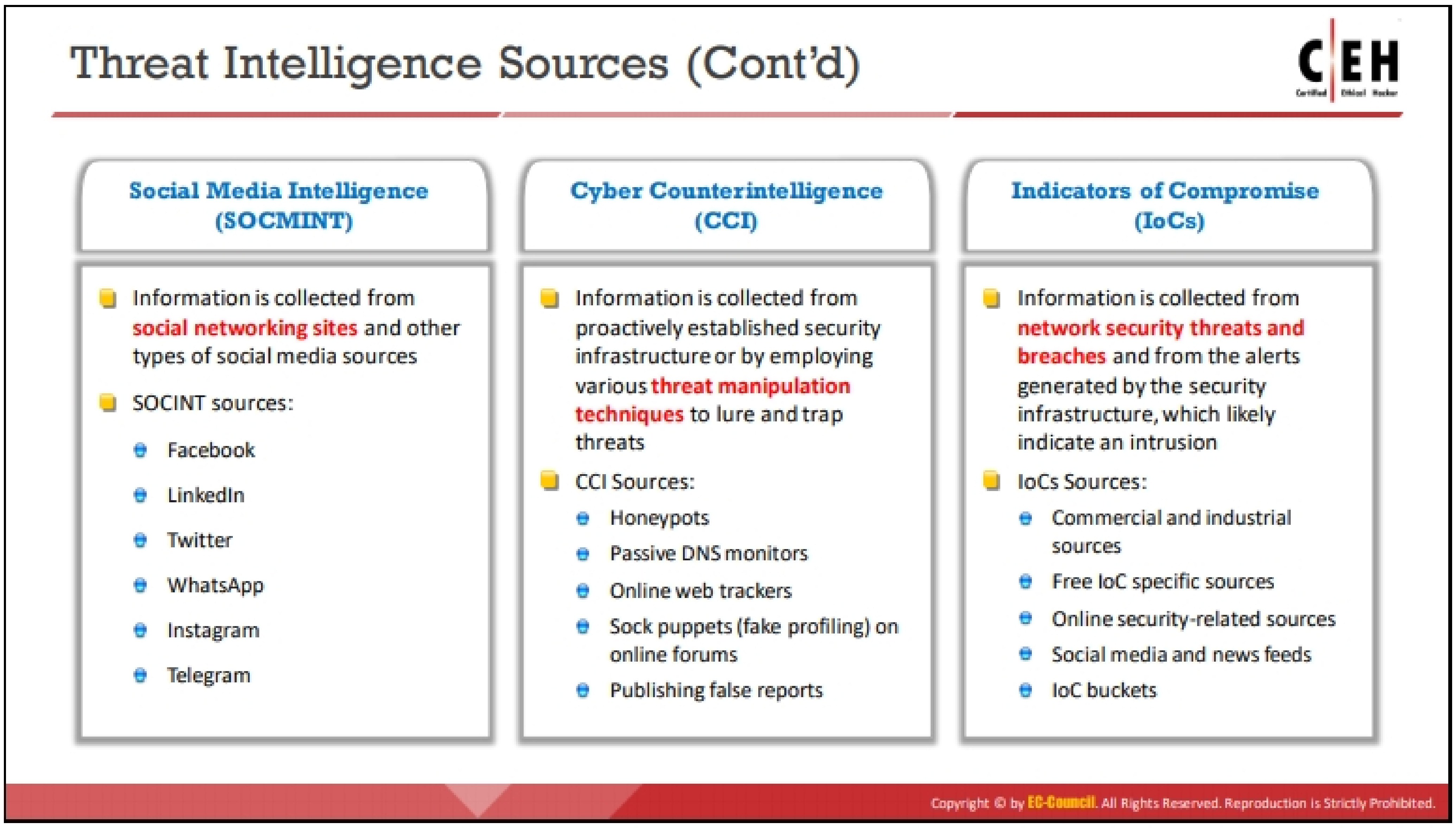
Covert Human Intelligence Sources (CHIS)

- Information is covertly collected from the target person by maintaining a **personal or other relationship** with the target person
- CHIS generally refers to a person or an agent under the Regulation of Investigatory Powers Act 2000 (RIPA), UK.
- CHIS sources are the persons targeted for information extraction

Financial Intelligence (FININT)

- Information is collected about the **adversary's financial affairs** and transactions that may involve tax evasions, money laundering, or other practices. This in turn provides information about the nature, capabilities, and intentions of the adversary
- FININT sources:
  - Financial Intelligence Unit (FIU)
  - Banks
  - SWIFT
  - Informal value transfer systems (IVTS)

Notes:



Threat Intelligence Sources (Cont'd)

Social Media Intelligence (SOCMINT)

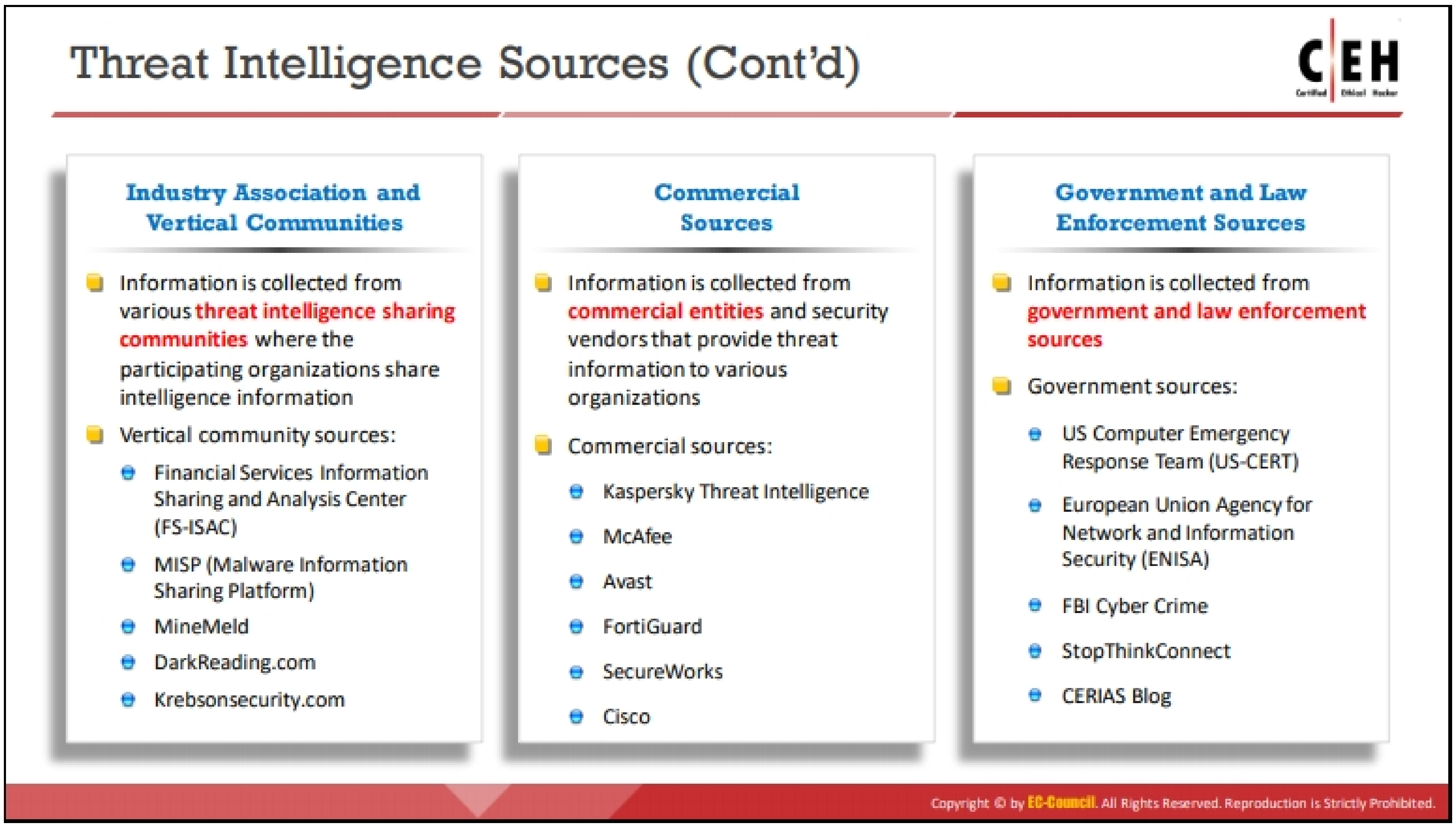
- Information is collected from **social networking sites** and other types of social media sources
- SOCINT sources:
  - Facebook
  - LinkedIn
  - Twitter
  - WhatsApp
  - Instagram
  - Telegram

Cyber Counterintelligence (CCI)

- Information is collected from proactively established security infrastructure or by employing various **threat manipulation techniques** to lure and trap threats
- CCI Sources:
  - Honeypots
  - Passive DNS monitors
  - Online web trackers
  - Sock puppets (fake profiling) on online forums
  - Publishing false reports

Indicators of Compromise (IoCs)

- Information is collected from **network security threats and breaches** and from the alerts generated by the security infrastructure, which likely indicate an intrusion
- IoCs Sources:
  - Commercial and industrial sources
  - Free IoC specific sources
  - Online security-related sources
  - Social media and news feeds
  - IoC buckets



Threat Intelligence Sources (Cont'd)

Industry Association and Vertical Communities

- Information is collected from various **threat intelligence sharing communities** where the participating organizations share intelligence information
- Vertical community sources:
  - Financial Services Information Sharing and Analysis Center (FS-ISAC)
  - MISP (Malware Information Sharing Platform)
  - MineMeld
  - DarkReading.com
  - Krebsonsecurity.com

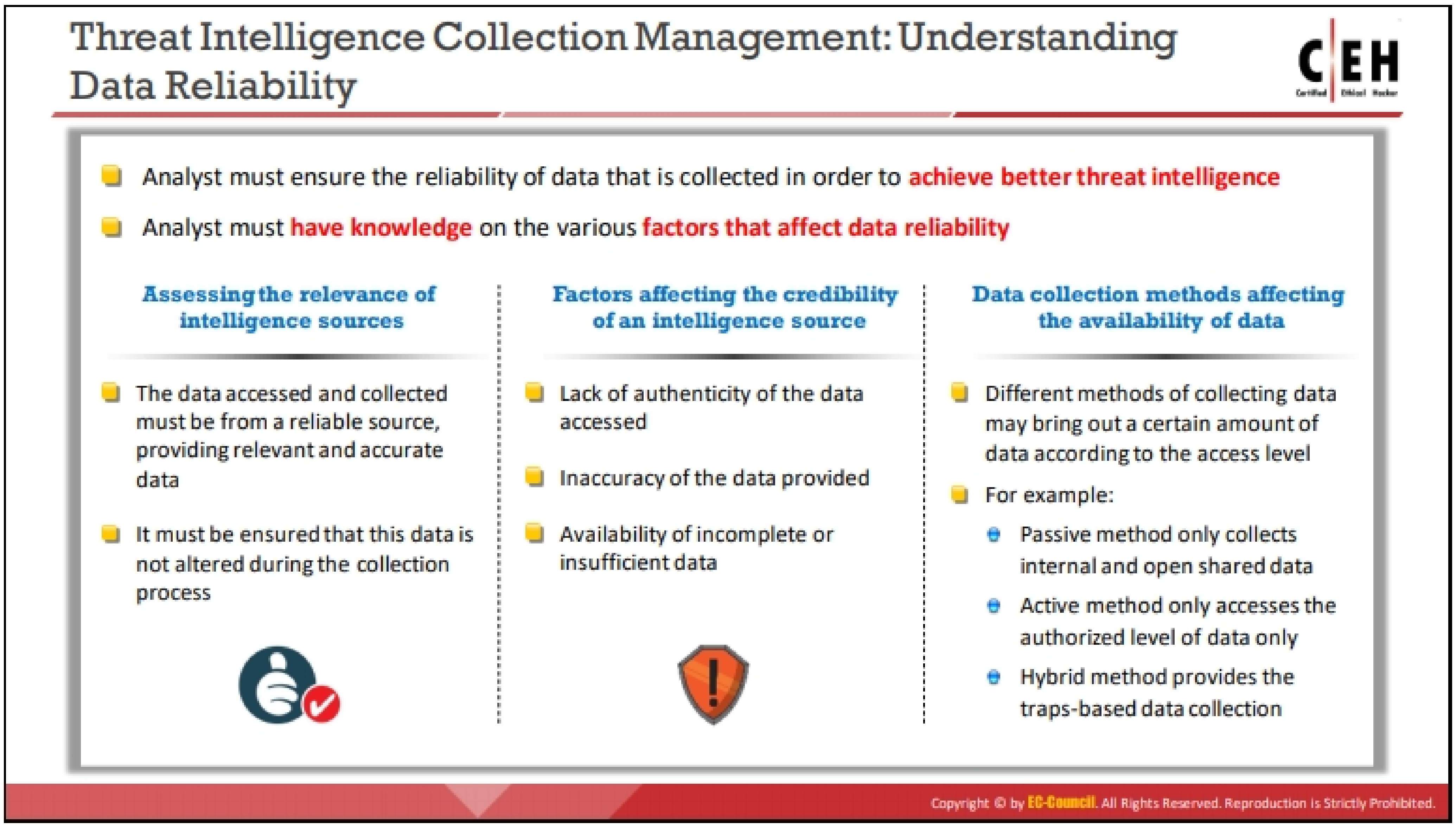
Commercial Sources

- Information is collected from **commercial entities** and security vendors that provide threat information to various organizations
- Commercial sources:
  - Kaspersky Threat Intelligence
  - McAfee
  - Avast
  - FortiGuard
  - SecureWorks
  - Cisco

Government and Law Enforcement Sources

- Information is collected from **government and law enforcement sources**
- Government sources:
  - US Computer Emergency Response Team (US-CERT)
  - European Union Agency for Network and Information Security (ENISA)
  - FBI Cyber Crime
  - StopThinkConnect
  - CERIAS Blog

Notes: ____



Threat Intelligence Collection Management: Understanding Data Reliability

- Analyst must ensure the reliability of data that is collected in order to **achieve better threat intelligence**
- Analyst must **have knowledge** on the various **factors that affect data reliability**

Assessing the relevance of intelligence sources

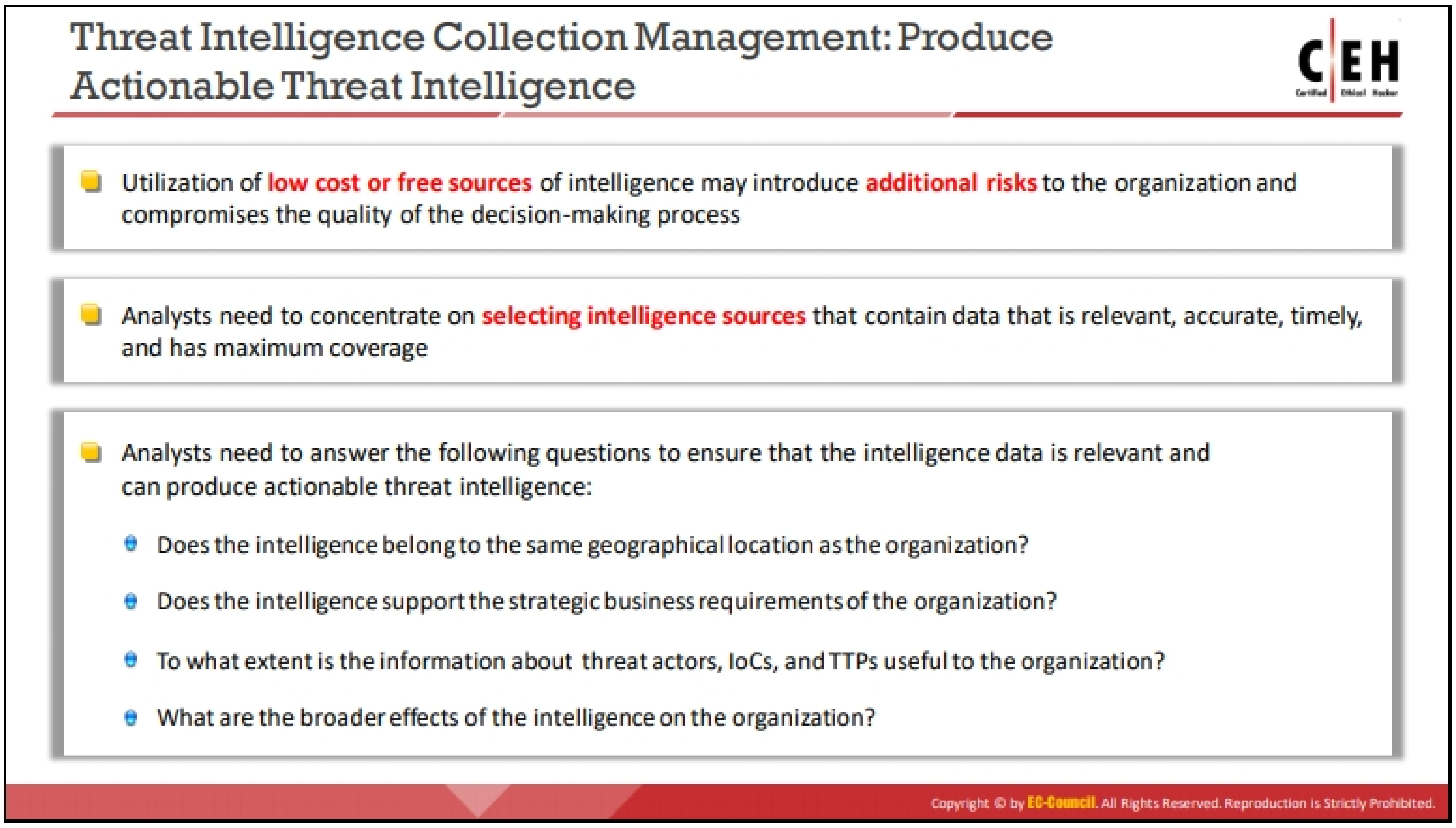
- The data accessed and collected must be from a reliable source, providing relevant and accurate data
- It must be ensured that this data is not altered during the collection process

Factors affecting the credibility of an intelligence source

- Lack of authenticity of the data accessed
- Inaccuracy of the data provided
- Availability of incomplete or insufficient data

Data collection methods affecting the availability of data

- Different methods of collecting data may bring out a certain amount of data according to the access level
- For example:
  - Passive method only collects internal and open shared data
  - Active method only accesses the authorized level of data only
  - Hybrid method provides the traps-based data collection



Threat Intelligence Collection Management: Produce Actionable Threat Intelligence

- Utilization of **low cost or free sources** of intelligence may introduce **additional risks** to the organization and compromises the quality of the decision-making process

- Analysts need to concentrate on **selecting intelligence sources** that contain data that is relevant, accurate, timely, and has maximum coverage

- Analysts need to answer the following questions to ensure that the intelligence data is relevant and can produce actionable threat intelligence:
  - Does the intelligence belong to the same geographical location as the organization?
  - Does the intelligence support the strategic business requirements of the organization?
  - To what extent is the information about threat actors, IoCs, and TTPs useful to the organization?
  - What are the broader effects of the intelligence on the organization?

Notes: ____

____

____

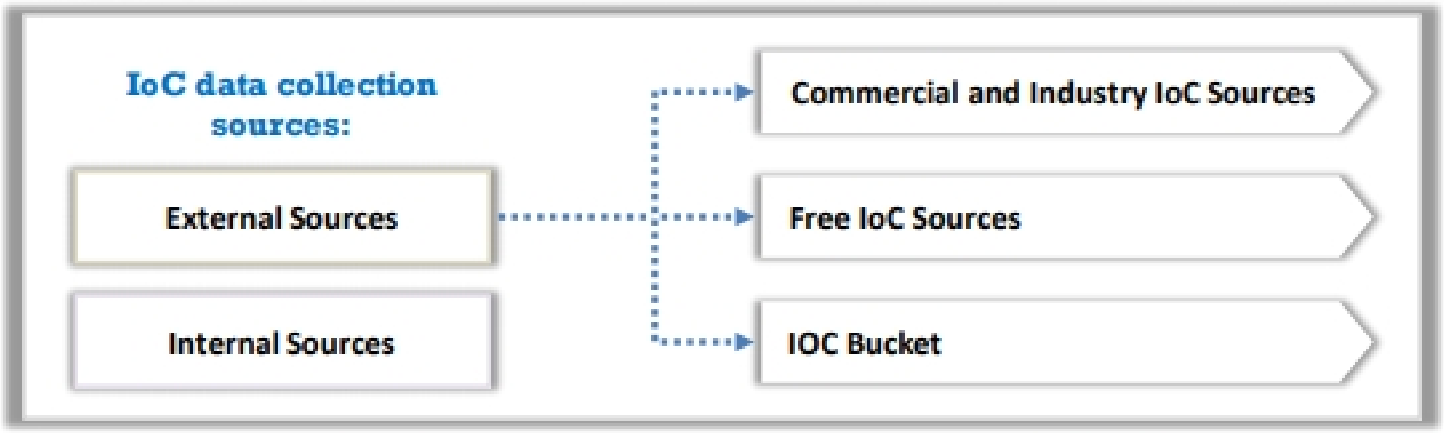
____

____

____

Collecting IoCs

- Indicators of Compromise (IoCs) are the **pieces of technical data** that are used for **building tactical threat intelligence**
- IoCs are the **clues or forensic evidence** that indicate a potential intrusion or malicious activity in an organizational network
- It comprises information regarding **suspicious or malicious activities** that is collected from various security establishments in a network infrastructure
- IoCs assist the analyst in knowing "**what happened**" in the attack and helps the analyst to observe the behavior and characteristics of malware



IoC data collection sources:

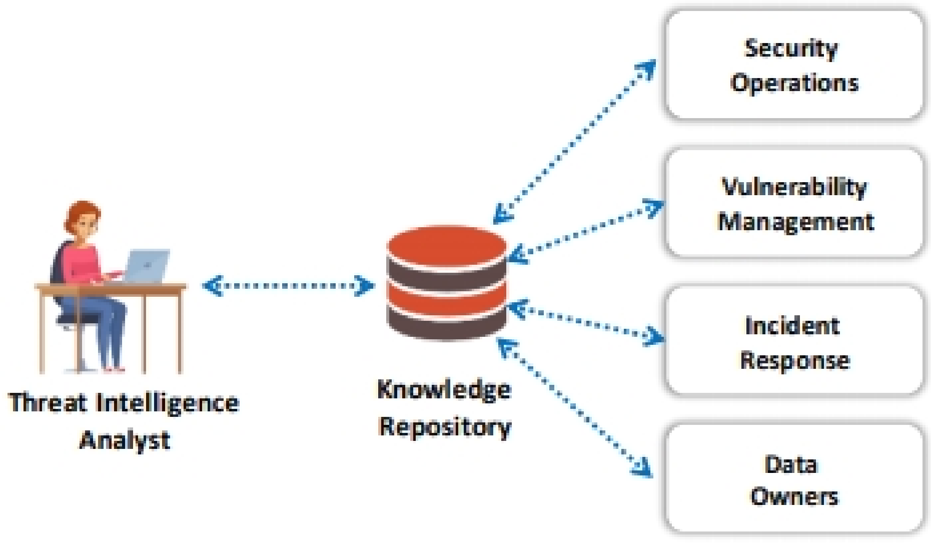
External Sources
Internal Sources
Commercial and Industry IoC Sources
Free IoC Sources
IOC Bucket

Create an Accessible Threat Knowledge Base

- A knowledge repository or **knowledge base** is an important tool for the management and dissemination of threat intelligence
- The repository helps analysts to document and share threat intelligence during the entire **threat collaboration environment**

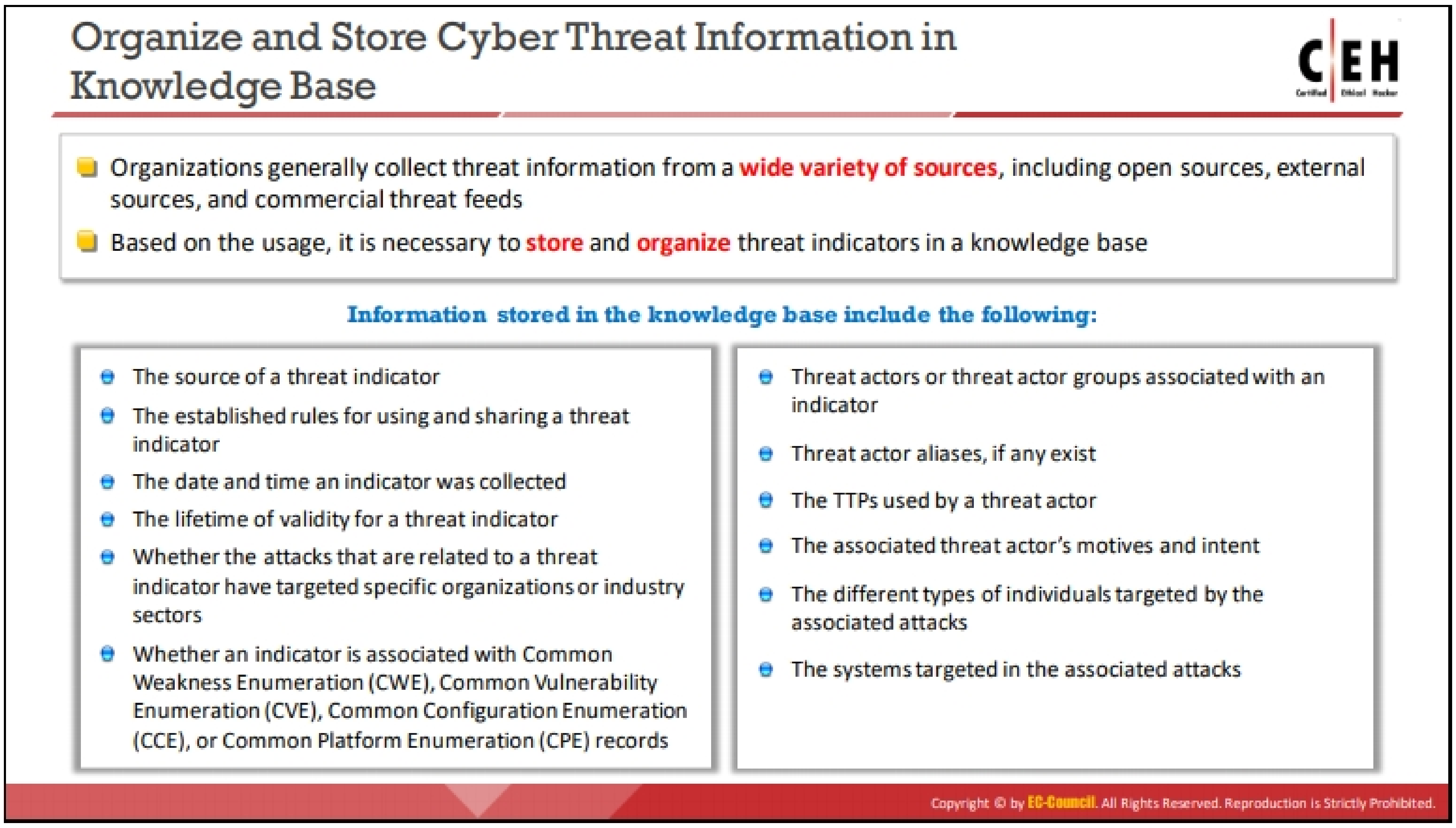
Threat knowledge repository must include:

- **Pivoting:** The ability to contextualize threat data and correlate related activities
- **Content Structuring:** The ability to store threat intelligence in a structured format
- **Data Management:** The ability to modify or delete past or irrelevant threat data
- **Protection Ranking:** The ability to apply protection ranking to sensitive data to ensure highly critical data is not shared with untrusted partners
- **News Feeds:** The ability to provide real-time news, alerts, briefings, and reports
- **Evaluating Performance:** The ability to evaluate past security metrics
- **Searchable Functionality:** The ability to query for and enrich indicators



Threat Intelligence Analyst
Knowledge Repository
Security Operations
Vulnerability Management
Incident Response
Data Owners

Notes: ____

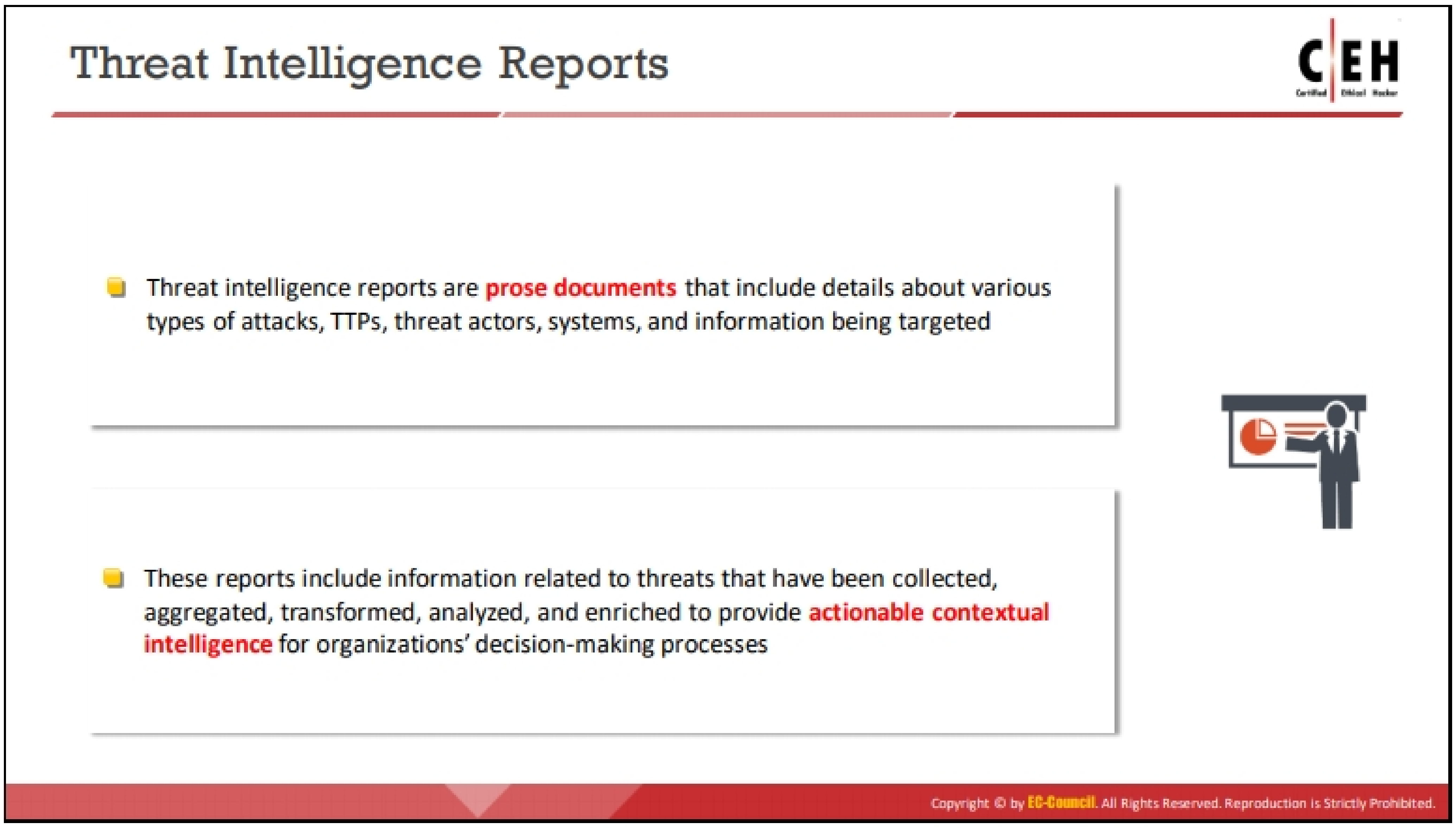


Organize and Store Cyber Threat Information in Knowledge Base

- Organizations generally collect threat information from a **wide variety of sources**, including open sources, external sources, and commercial threat feeds
- Based on the usage, it is necessary to **store** and **organize** threat indicators in a knowledge base

Information stored in the knowledge base include the following:

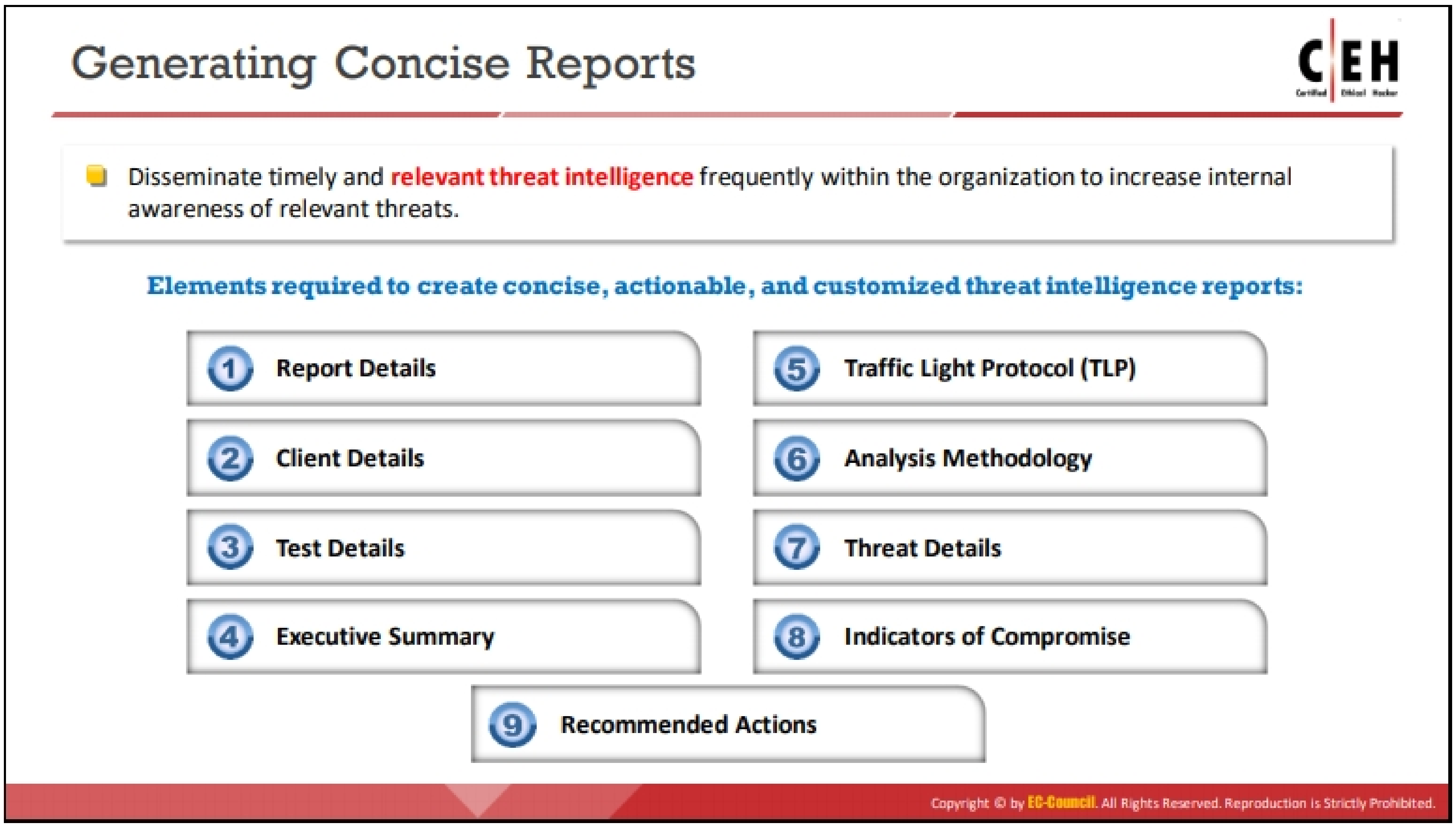
- The source of a threat indicator
- The established rules for using and sharing a threat indicator
- The date and time an indicator was collected
- The lifetime of validity for a threat indicator
- Whether the attacks that are related to a threat indicator have targeted specific organizations or industry sectors
- Whether an indicator is associated with Common Weakness Enumeration (CWE), Common Vulnerability Enumeration (CVE), Common Configuration Enumeration (CCE), or Common Platform Enumeration (CPE) records
- Threat actors or threat actor groups associated with an indicator
- Threat actor aliases, if any exist
- The TTPs used by a threat actor
- The associated threat actor's motives and intent
- The different types of individuals targeted by the associated attacks
- The systems targeted in the associated attacks



Threat Intelligence Reports

- Threat intelligence reports are **prose documents** that include details about various types of attacks, TTPs, threat actors, systems, and information being targeted
- These reports include information related to threats that have been collected, aggregated, transformed, analyzed, and enriched to provide **actionable contextual intelligence** for organizations' decision-making processes

Notes:

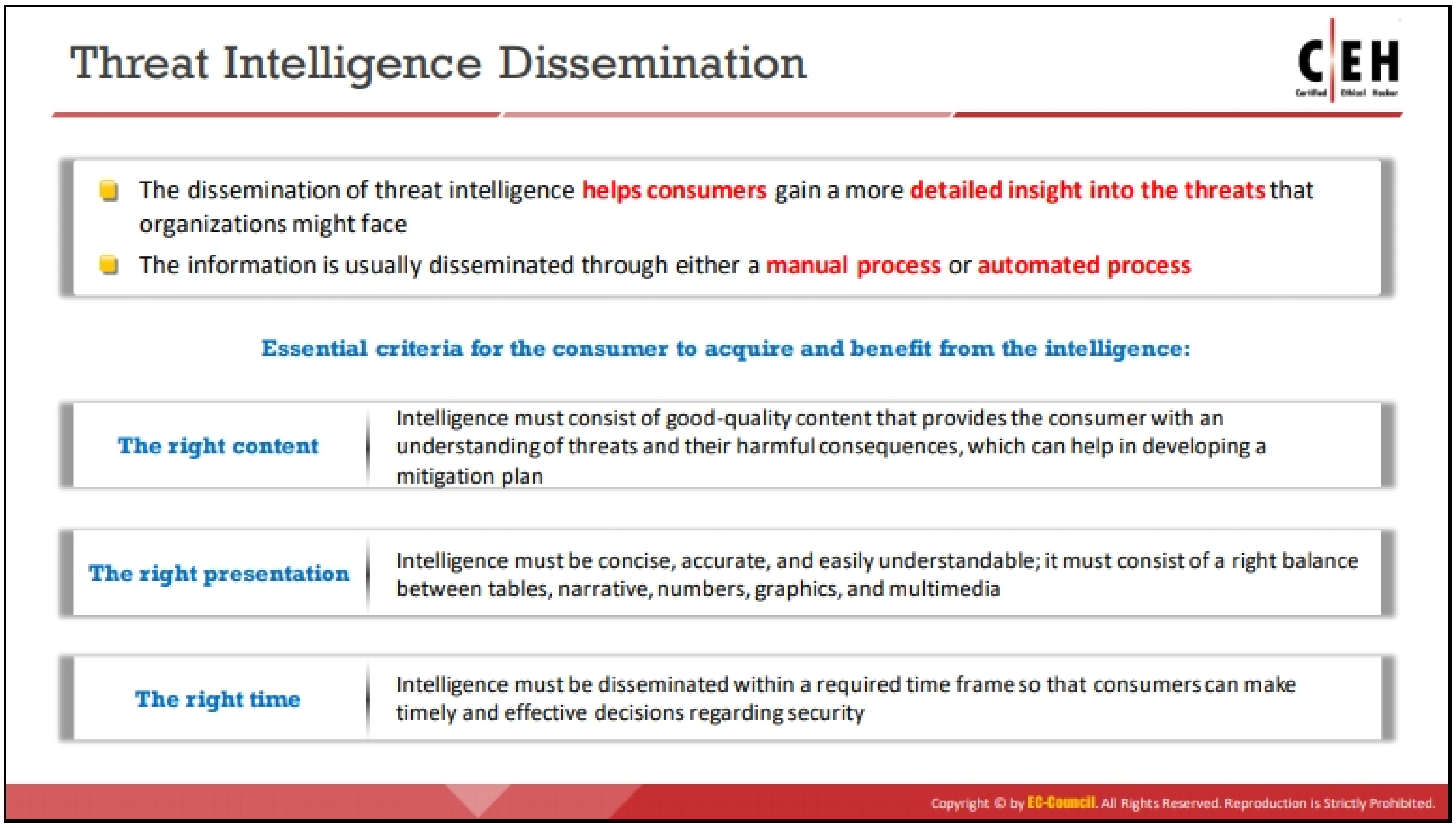


Generating Concise Reports

- Disseminate timely and **relevant threat intelligence** frequently within the organization to increase internal awareness of relevant threats.

Elements required to create concise, actionable, and customized threat intelligence reports:

1. **Report Details**
2. **Client Details**
3. **Test Details**
4. **Executive Summary**
5. **Traffic Light Protocol (TLP)**
6. **Analysis Methodology**
7. **Threat Details**
8. **Indicators of Compromise**
9. **Recommended Actions**



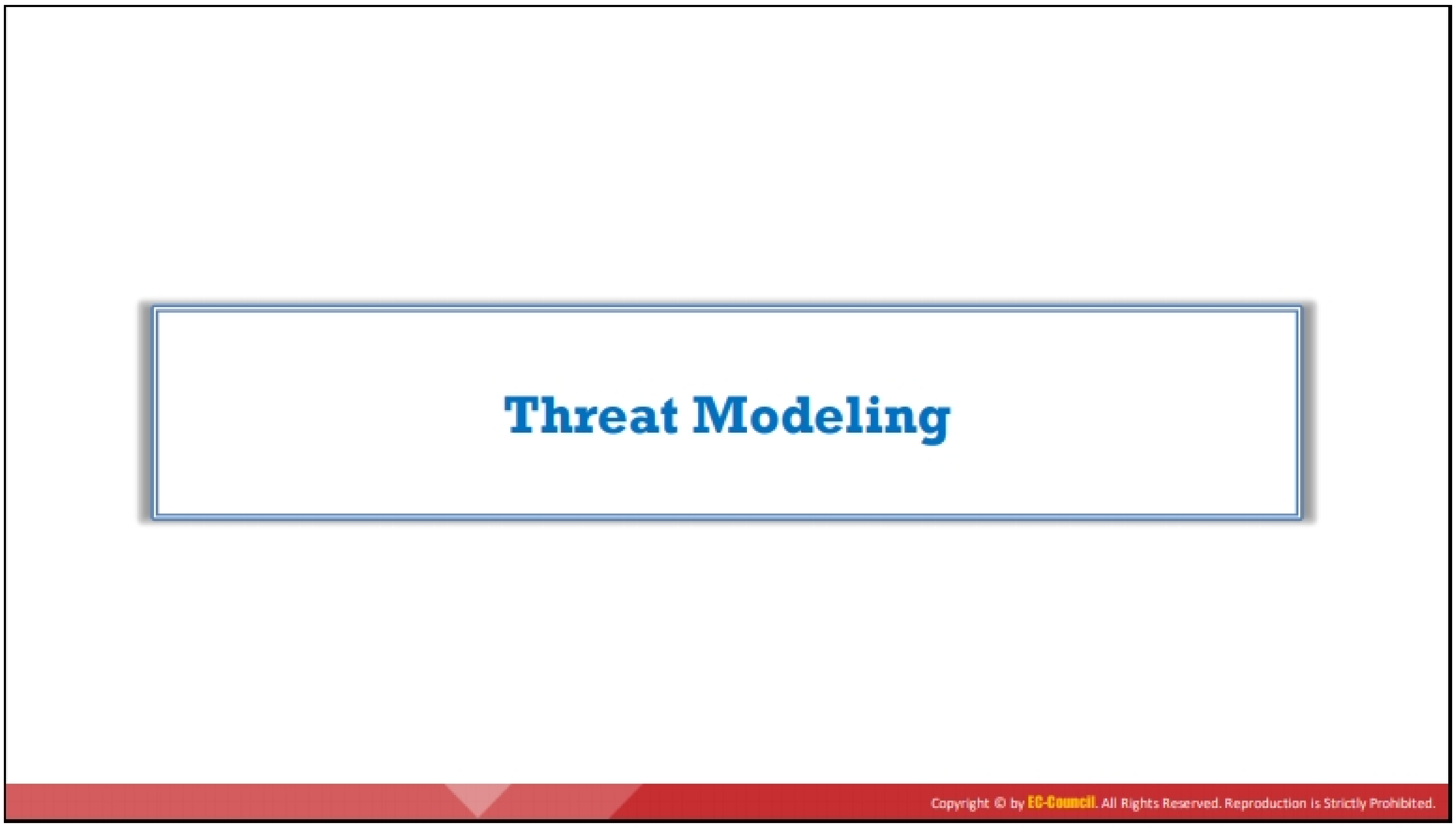
Threat Intelligence Dissemination

- The dissemination of threat intelligence **helps consumers** gain a more **detailed insight into the threats** that organizations might face
- The information is usually disseminated through either a **manual process** or **automated process**

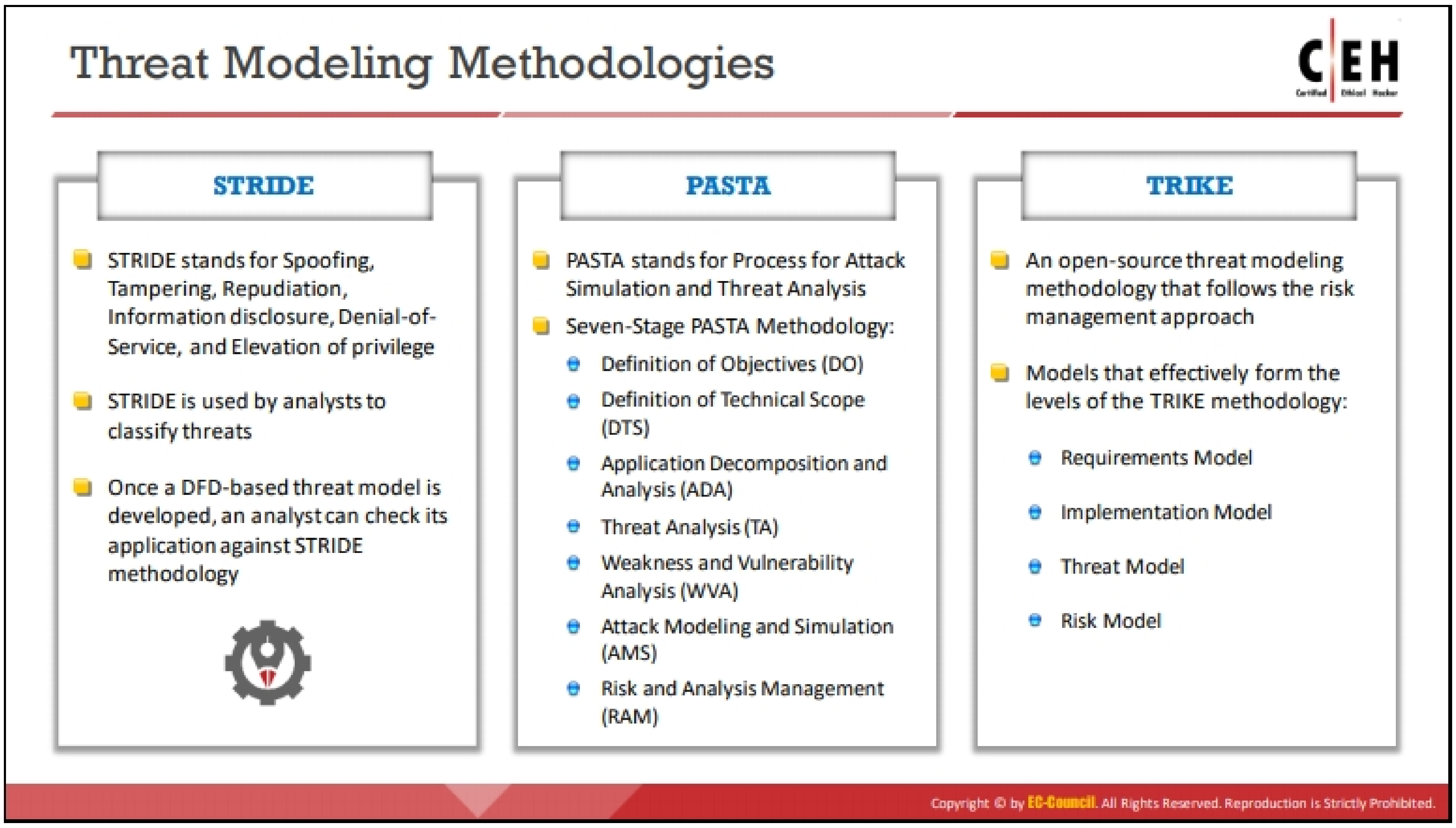
Essential criteria for the consumer to acquire and benefit from the intelligence:

The right content	Intelligence must consist of good-quality content that provides the consumer with an understanding of threats and their harmful consequences, which can help in developing a mitigation plan
The right presentation	Intelligence must be concise, accurate, and easily understandable; it must consist of a right balance between tables, narrative, numbers, graphics, and multimedia
The right time	Intelligence must be disseminated within a required time frame so that consumers can make timely and effective decisions regarding security

Notes: ____



Threat Modeling



Threat Modeling Methodologies

STRIDE

- STRIDE stands for Spoofing, Tampering, Repudiation, Information disclosure, Denial-of-Service, and Elevation of privilege
- STRIDE is used by analysts to classify threats
- Once a DFD-based threat model is developed, an analyst can check its application against STRIDE methodology

PASTA

- PASTA stands for Process for Attack Simulation and Threat Analysis
- Seven-Stage PASTA Methodology:
  - Definition of Objectives (DO)
  - Definition of Technical Scope (DTS)
  - Application Decomposition and Analysis (ADA)
  - Threat Analysis (TA)
  - Weakness and Vulnerability Analysis (WVA)
  - Attack Modeling and Simulation (AMS)
  - Risk and Analysis Management (RAM)

TRIKE

- An open-source threat modeling methodology that follows the risk management approach
- Models that effectively form the levels of the TRIKE methodology:
  - Requirements Model
  - Implementation Model
  - Threat Model
  - Risk Model

Notes: ____

Threat Modeling Methodologies (Cont'd)

VAST

- VAST stands for Visual, Agile, and Simple Threat modeling
- The primary objective of developing this methodology is to scale the threat modeling across the infrastructure and entire DevOps portfolio
- Based on the practical approach in the development of the following threat models:
  - Application Threat Model
  - Operational Threat Model

DREAD

- DREAD stands for Damage, Reproducibility, Exploitability, Affected Users, and Discoverability
- A sorting scheme for calculating, comparing, and ranking the possible extent of threat for each assessed risk
- The DREAD formula for calculating the risk value:

  Risk = (Damage + Reproducibility + Exploitability + Affected Users + Discoverability)/5

OCTAVE

- OCTAVE stands for Operationally Critical Threat, Asset, and Vulnerability Evaluation
- Three stages of OCTAVE methodology:
  - Build Asset-Based Threat Profiles
  - Identify Infrastructure Vulnerabilities
  - Develop Security Strategy and Plans

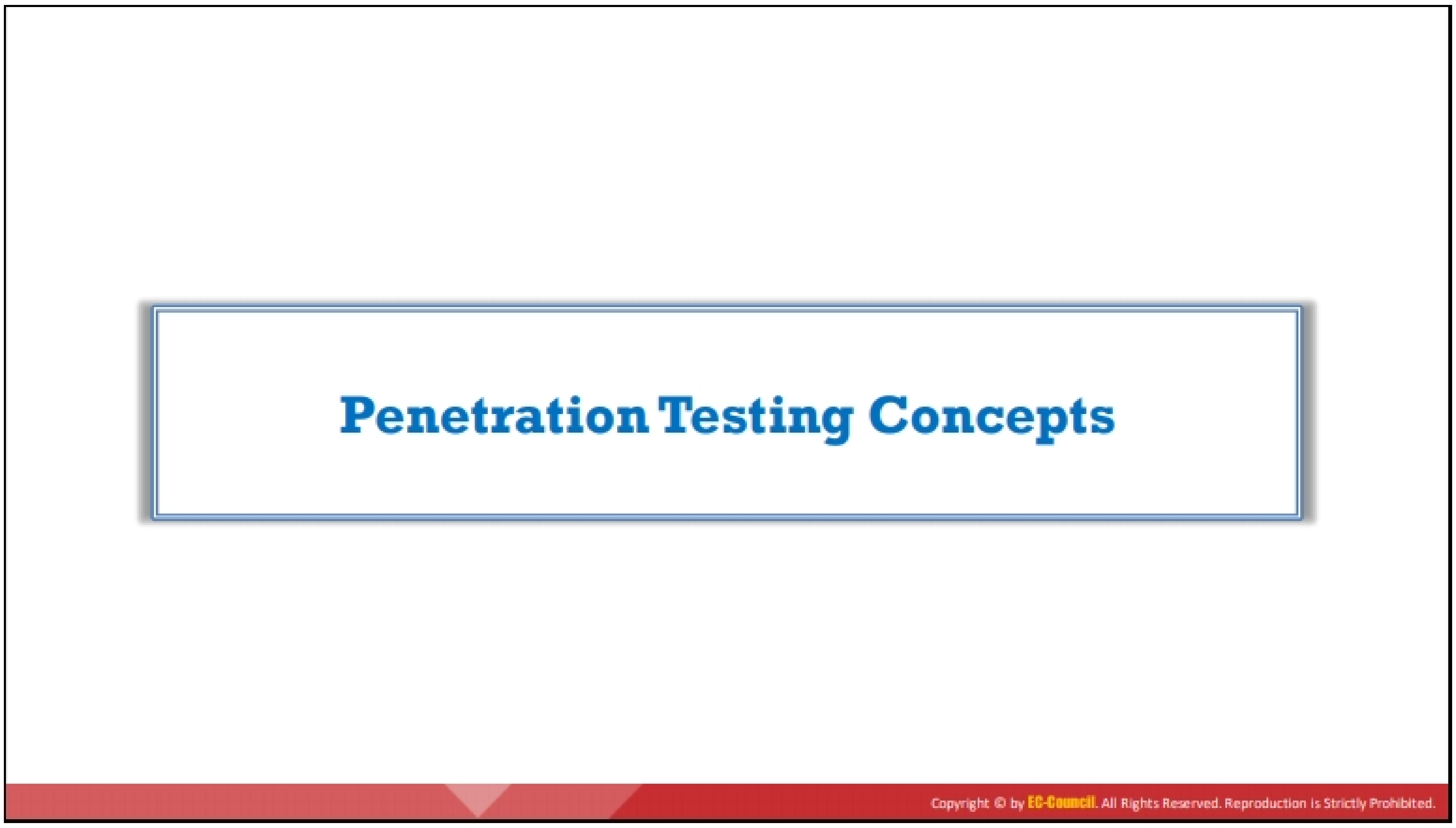
Threat Profiling and Attribution

- Threat Profiling and Attribution involves collecting information about threat actors and **building an analytic profile of the adversary**
- It describes the **adversary's technological details**, goals, and motives which can be resourceful in building a strong countermeasure

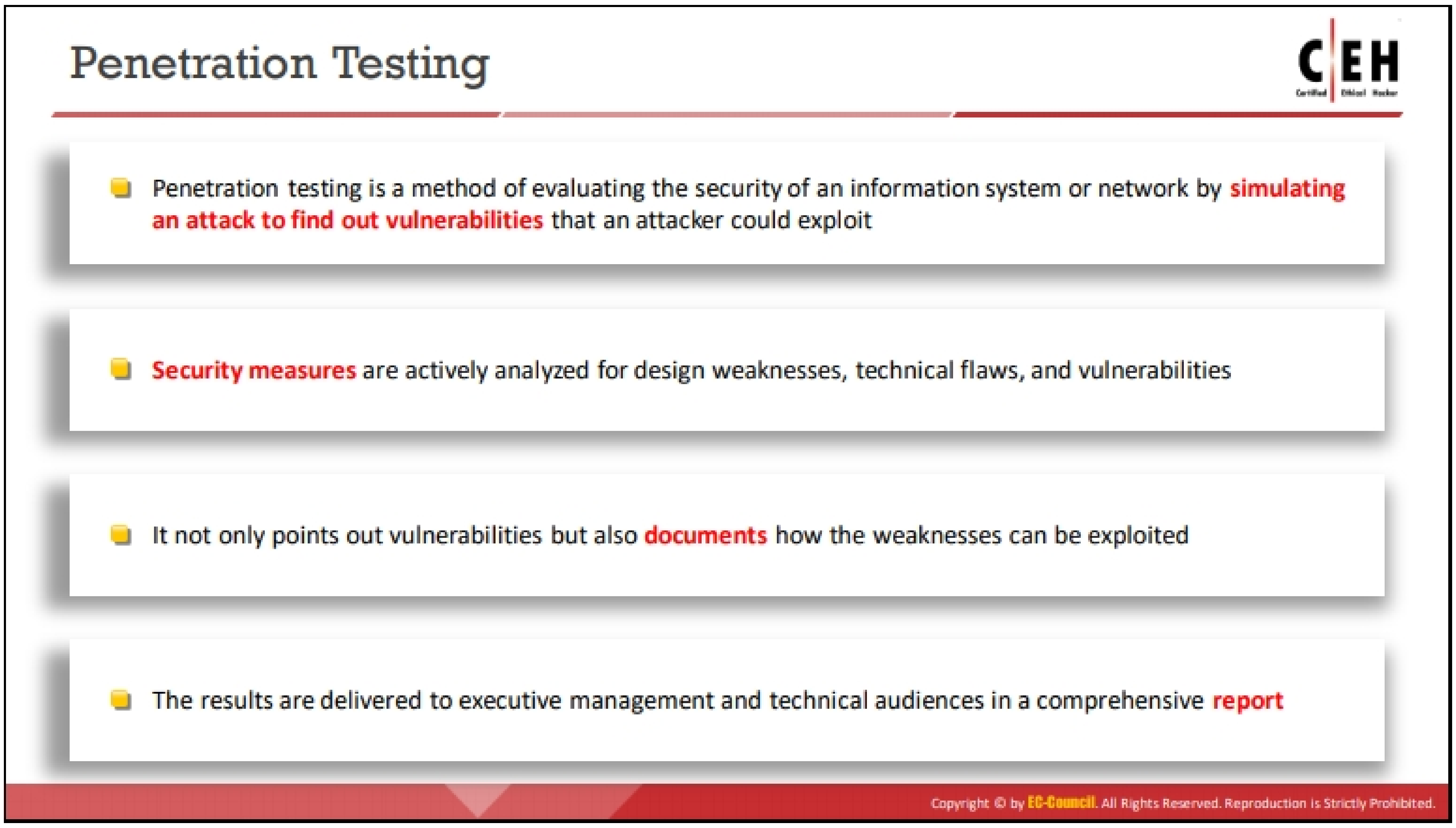
The threat profile can be created to include the details of the following attributes:

1. **Description**
2. **Motive**
3. **Intent**
4. **Capability**
5. **Ownership Detail**
6. **Target Detail**
7. **Operating Methods**
8. **Objective**

Notes:



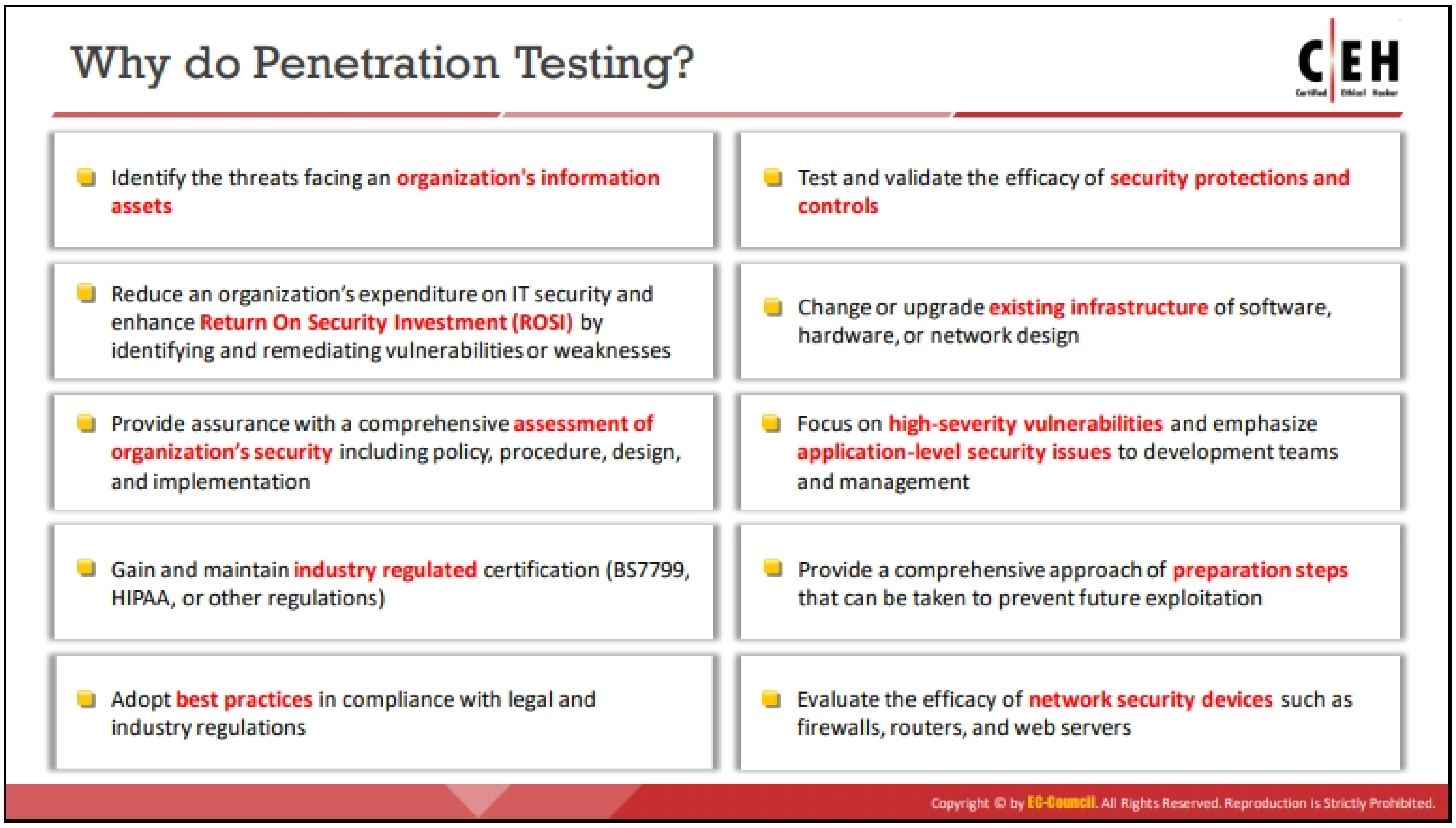
Penetration Testing Concepts



Penetration Testing

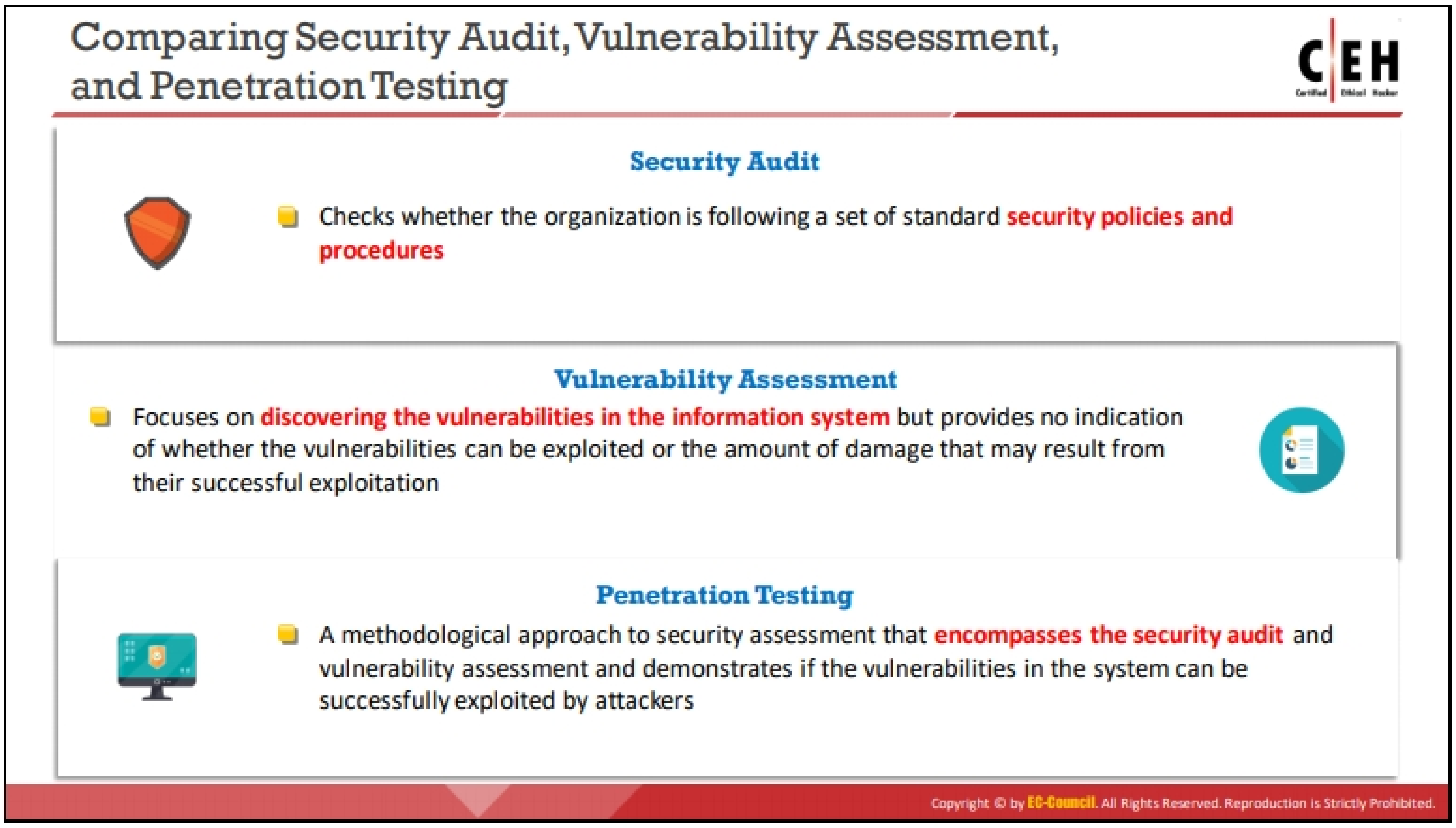
- Penetration testing is a method of evaluating the security of an information system or network by **simulating an attack to find out vulnerabilities** that an attacker could exploit
- **Security measures** are actively analyzed for design weaknesses, technical flaws, and vulnerabilities
- It not only points out vulnerabilities but also **documents** how the weaknesses can be exploited
- The results are delivered to executive management and technical audiences in a comprehensive **report**

Notes: ____



Why do Penetration Testing?

- Identify the threats facing an **organization's information assets**
- Test and validate the efficacy of **security protections and controls**
- Reduce an organization's expenditure on IT security and enhance **Return On Security Investment (ROSI)** by identifying and remediating vulnerabilities or weaknesses
- Change or upgrade **existing infrastructure** of software, hardware, or network design
- Provide assurance with a comprehensive **assessment of organization's security** including policy, procedure, design, and implementation
- Focus on **high-severity vulnerabilities** and emphasize **application-level security issues** to development teams and management
- Gain and maintain **industry regulated** certification (BS7799, HIPAA, or other regulations)
- Provide a comprehensive approach of **preparation steps** that can be taken to prevent future exploitation
- Adopt **best practices** in compliance with legal and industry regulations
- Evaluate the efficacy of **network security devices** such as firewalls, routers, and web servers



Comparing Security Audit, Vulnerability Assessment, and Penetration Testing

Security Audit

- Checks whether the organization is following a set of standard **security policies and procedures**

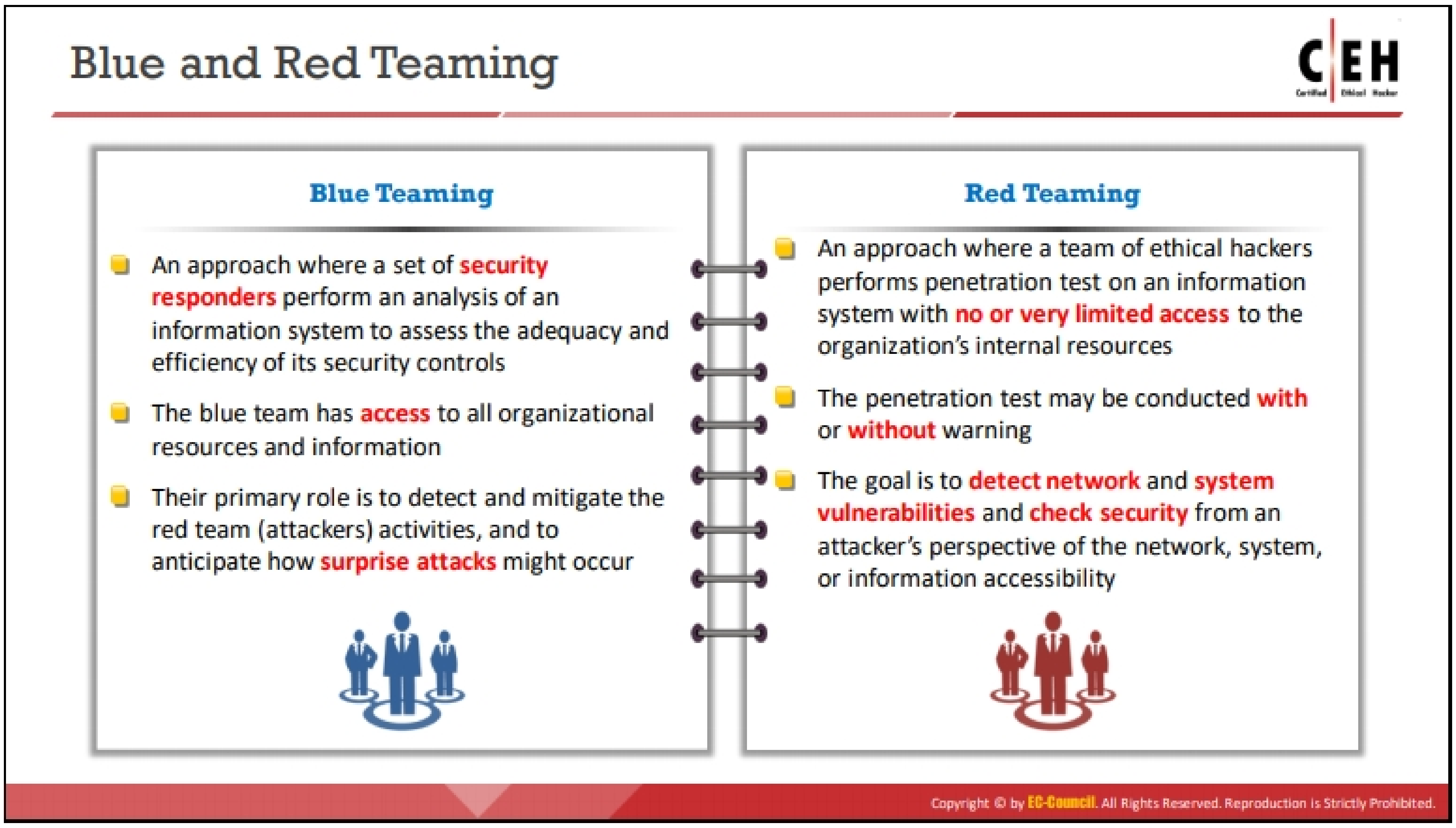
Vulnerability Assessment

- Focuses on **discovering the vulnerabilities in the information system** but provides no indication of whether the vulnerabilities can be exploited or the amount of damage that may result from their successful exploitation

Penetration Testing

- A methodological approach to security assessment that **encompasses the security audit** and vulnerability assessment and demonstrates if the vulnerabilities in the system can be successfully exploited by attackers

Notes: ____



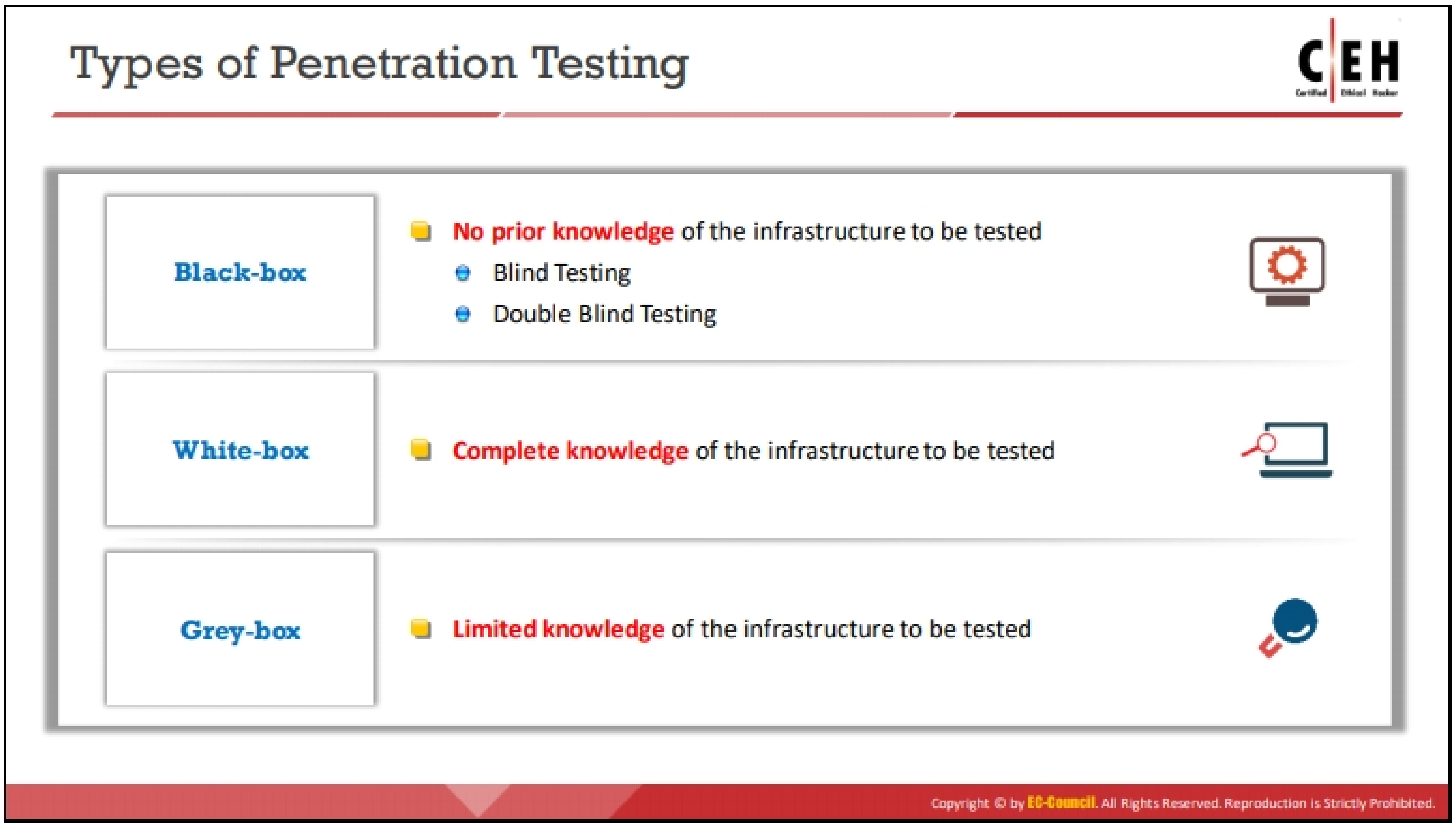
Blue and Red Teaming

Blue Teaming

- An approach where a set of **security responders** perform an analysis of an information system to assess the adequacy and efficiency of its security controls
- The blue team has **access** to all organizational resources and information
- Their primary role is to detect and mitigate the red team (attackers) activities, and to anticipate how **surprise attacks** might occur

Red Teaming

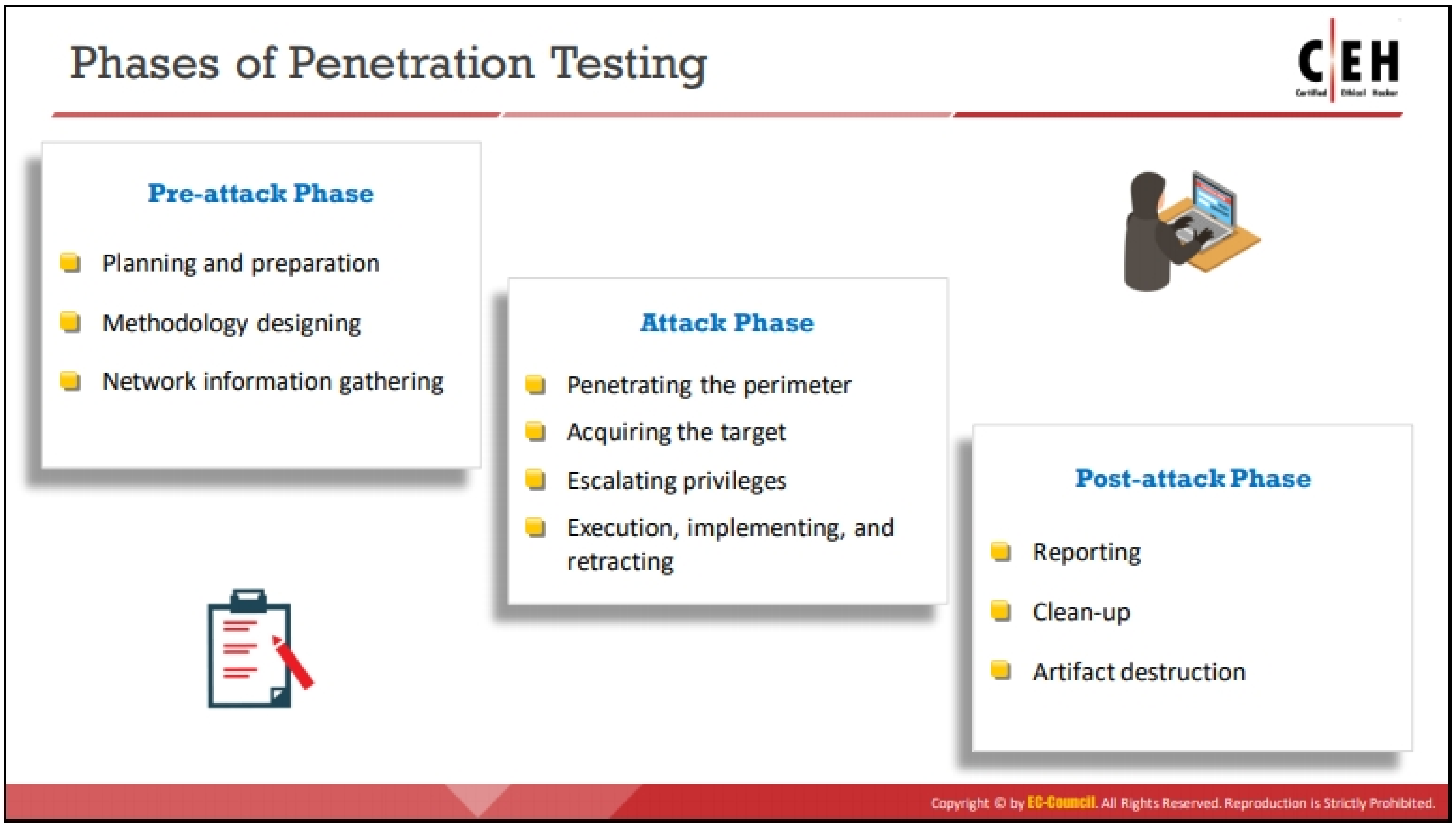
- An approach where a team of ethical hackers performs penetration test on an information system with **no or very limited access** to the organization's internal resources
- The penetration test may be conducted **with** or **without** warning
- The goal is to **detect network** and **system vulnerabilities** and **check security** from an attacker's perspective of the network, system, or information accessibility



Types of Penetration Testing

Black-box	**No prior knowledge** of the infrastructure to be tested Blind Testing Double Blind Testing
White-box	**Complete knowledge** of the infrastructure to be tested
Grey-box	**Limited knowledge** of the infrastructure to be tested

Notes: ____________________



Phases of Penetration Testing

Pre-attack Phase

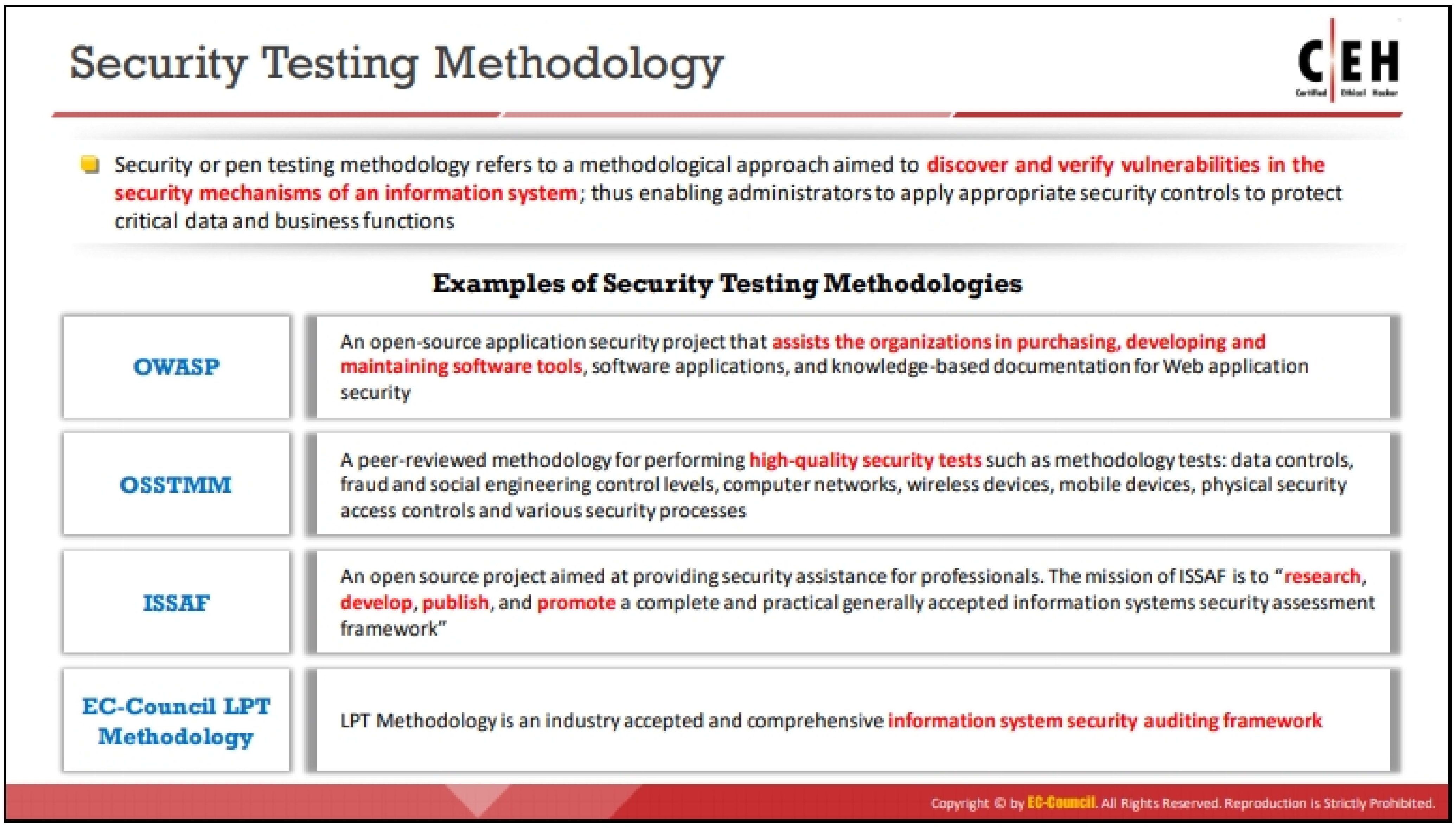
- Planning and preparation
- Methodology designing
- Network information gathering

Attack Phase

- Penetrating the perimeter
- Acquiring the target
- Escalating privileges
- Execution, implementing, and retracting

Post-attack Phase

- Reporting
- Clean-up
- Artifact destruction



Security Testing Methodology

- Security or pen testing methodology refers to a methodological approach aimed to discover and verify vulnerabilities in the security mechanisms of an information system; thus enabling administrators to apply appropriate security controls to protect critical data and business functions

Examples of Security Testing Methodologies

OWASP	An open-source application security project that assists the organizations in purchasing, developing and maintaining software tools, software applications, and knowledge-based documentation for Web application security
OSSTMM	A peer-reviewed methodology for performing high-quality security tests such as methodology tests: data controls, fraud and social engineering control levels, computer networks, wireless devices, mobile devices, physical security access controls and various security processes
ISSAF	An open source project aimed at providing security assistance for professionals. The mission of ISSAF is to "research, develop, publish, and promote a complete and practical generally accepted information systems security assessment framework"
EC-Council LPT Methodology	LPT Methodology is an industry accepted and comprehensive information system security auditing framework

Notes: ____

____

____

____

____

____

Risks Associated with Penetration Testing

- Careful engagement, planning, and execution is required to avoid any risks associated with penetration testing
- There are certain risks that organizations may face when they plan to conduct a penetration test

- Some of the risks arising from penetration testing are:
  - Testers can gain access to the protected or sensitive data after a successful penetration test attempt
  - Testers can obtain information about the vulnerabilities existing in the organizational infrastructure
  - DoS penetration testing can bring the organization's services down
  - Using certain pretexts in social engineering, a penetration attempt can make employees feel uneasy

- Organizations can avoid such risks by signing NDA and other legal documents, which include details about what is allowed and not allowed to the penetration testing team

Types of Risks Arising During Penetration Testing

- During the penetration test, some of the activities may pose certain risks and cause the organization unwanted situations such as a denial of service conditions, being locked out critical accounts, or crashing critical servers and applications

Types of risks that come with penetration testing

Technical Risks:

- Directly arises with targets in the production environment
- Example include:
  - Failure of the target
  - Disruption of service
  - Loss or exposure of sensitive data

Organizational Risks:

- Can come as a side effect of penetration testing
- Examples include:
  - A repetitive and unwanted triggering in the incident handling processes of the organization
  - Negligence towards monitoring and responding to incidents during or after a pen test
  - A disruption in business continuity
  - Loss of reputation

Legal Risks:

- Arise from Legal obligations
- Examples include:
  - Violation of laws, clauses in ROE

Notes: ____

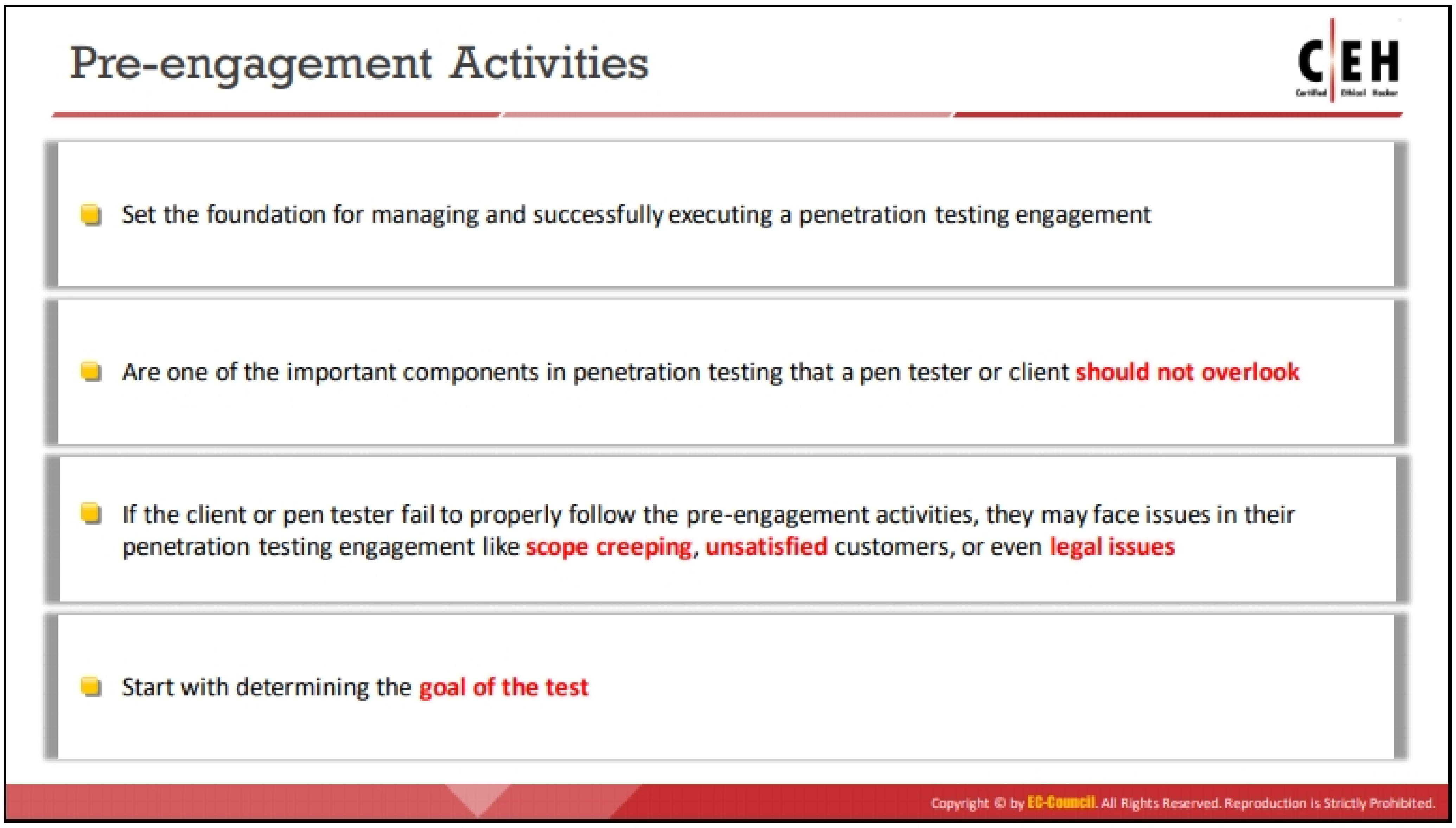
____

____

____

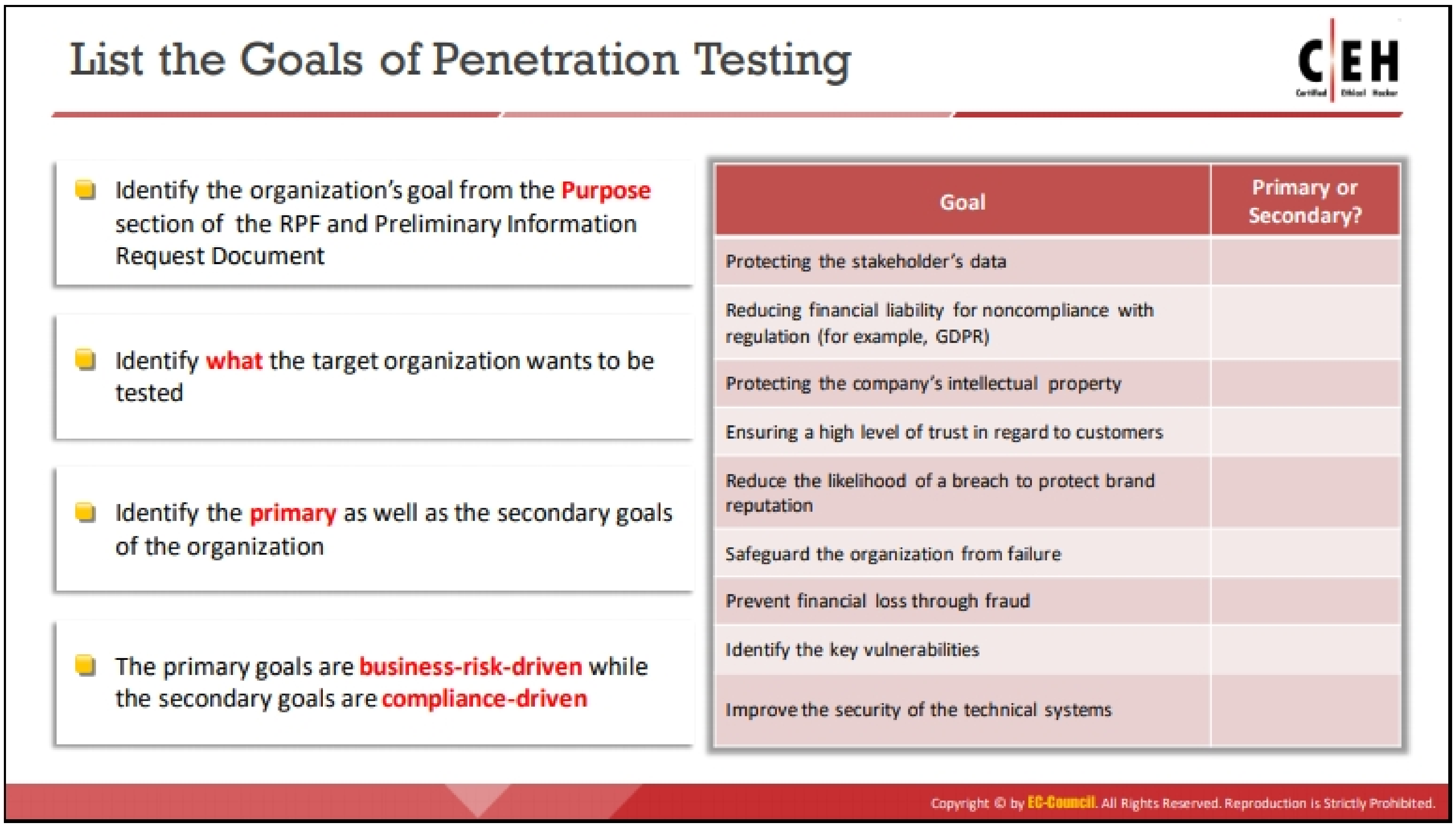
____

____



Pre-engagement Activities

- Set the foundation for managing and successfully executing a penetration testing engagement
- Are one of the important components in penetration testing that a pen tester or client **should not overlook**
- If the client or pen tester fail to properly follow the pre-engagement activities, they may face issues in their penetration testing engagement like **scope creeping**, **unsatisfied** customers, or even **legal issues**
- Start with determining the **goal of the test**



List the Goals of Penetration Testing

- Identify the organization's goal from the **Purpose** section of the RPF and Preliminary Information Request Document
- Identify **what** the target organization wants to be tested
- Identify the **primary** as well as the secondary goals of the organization
- The primary goals are **business-risk-driven** while the secondary goals are **compliance-driven**

Goal	Primary or Secondary?
Protecting the stakeholder's data	
Reducing financial liability for noncompliance with regulation (for example, GDPR)	
Protecting the company's intellectual property	
Ensuring a high level of trust in regard to customers	
Reduce the likelihood of a breach to protect brand reputation	
Safeguard the organization from failure	
Prevent financial loss through fraud	
Identify the key vulnerabilities	
Improve the security of the technical systems	

Notes: ____

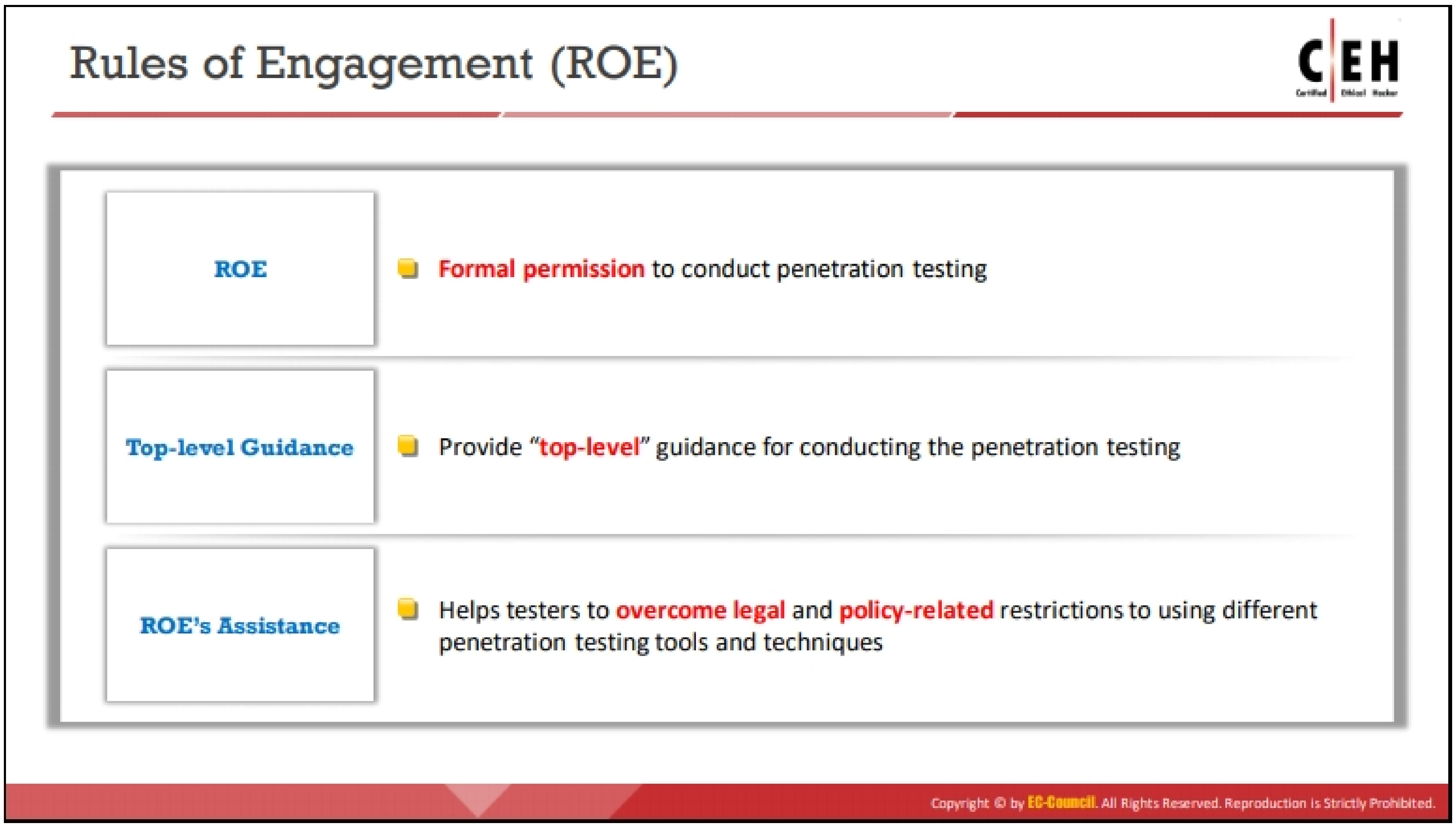
____

____

____

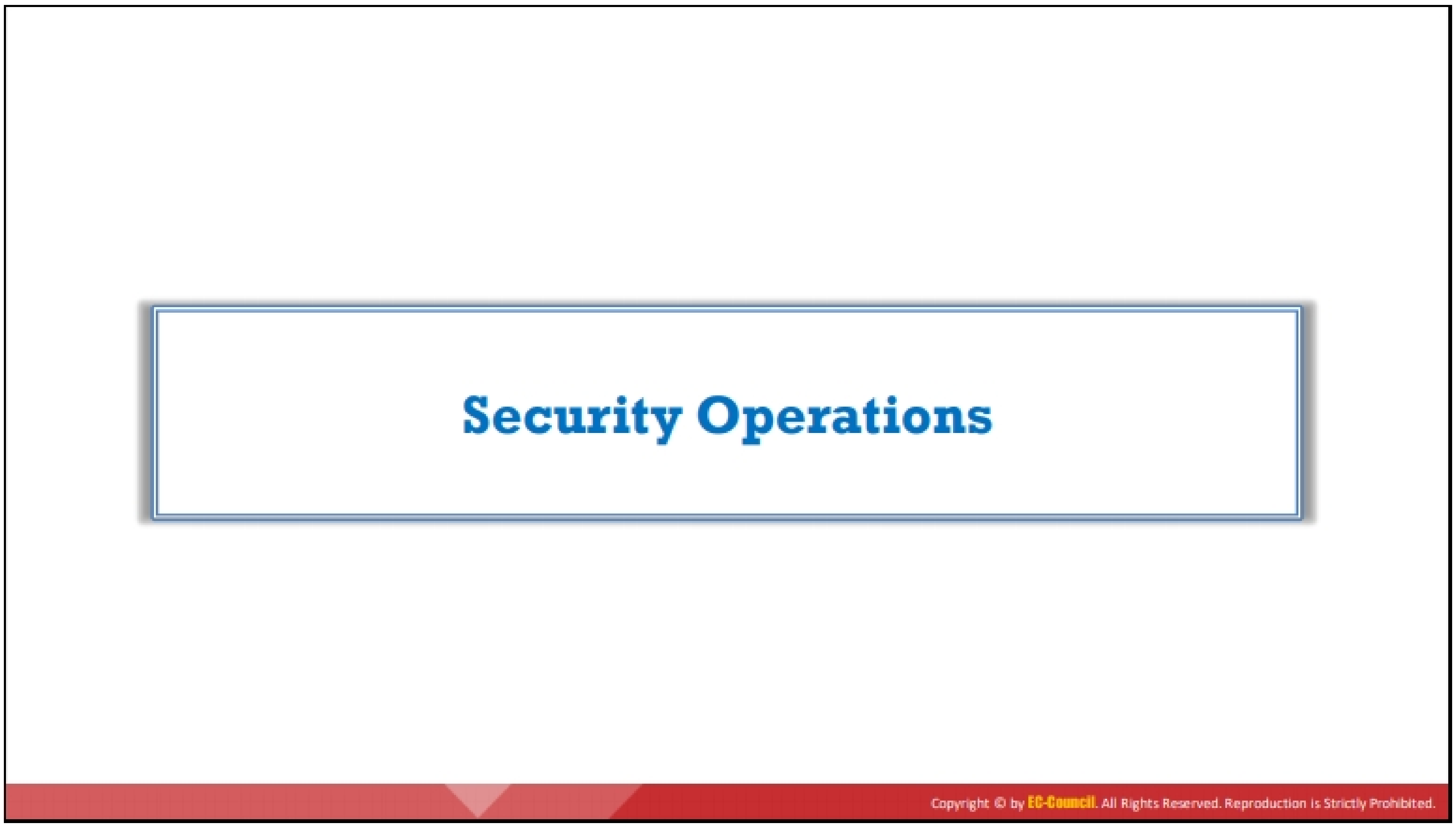
____

____



Rules of Engagement (ROE)

ROE	Formal permission to conduct penetration testing
Top-level Guidance	Provide "top-level" guidance for conducting the penetration testing
ROE's Assistance	Helps testers to overcome legal and policy-related restrictions to using different penetration testing tools and techniques



Security Operations

Notes: ____

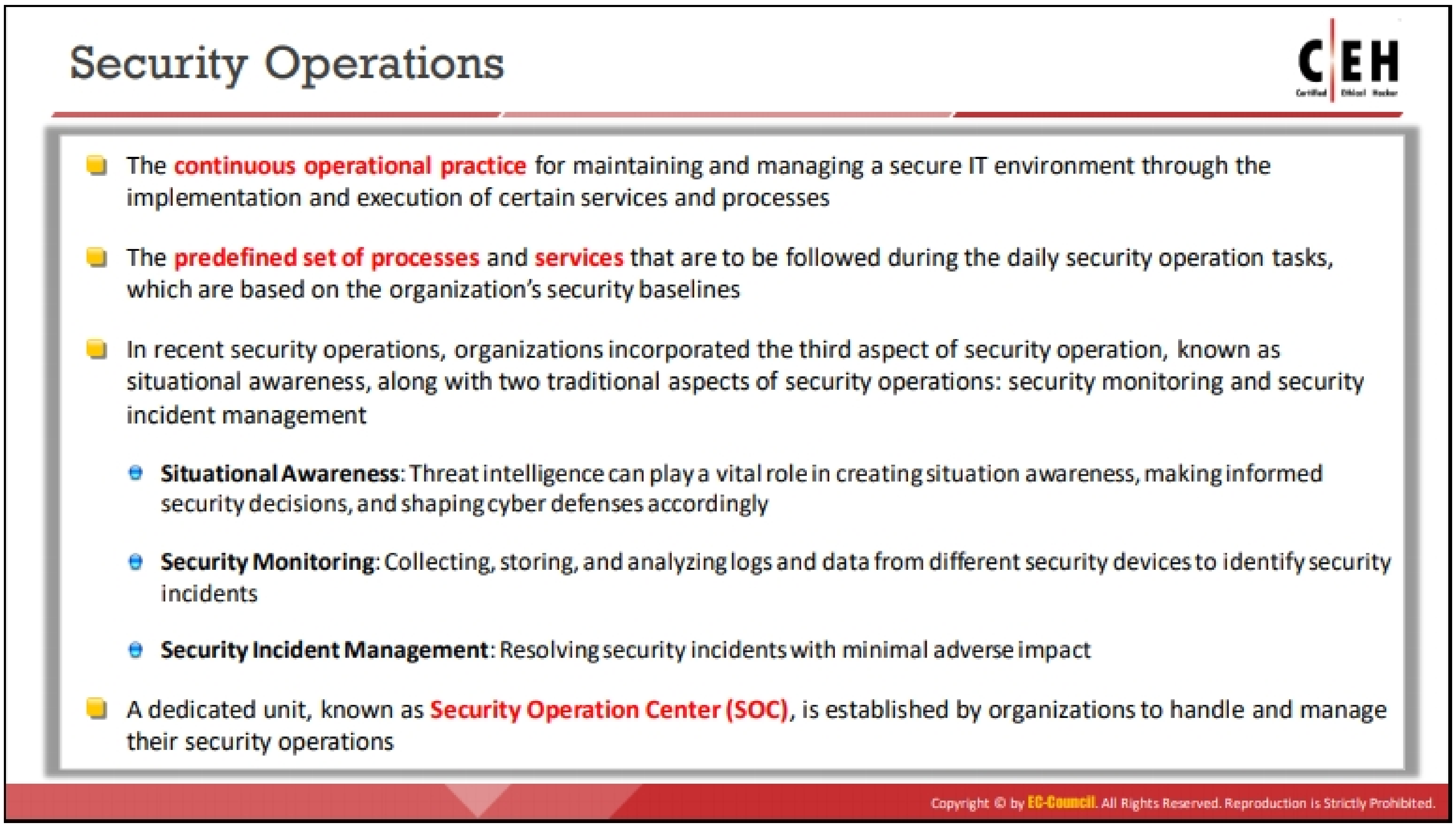
____

____

____

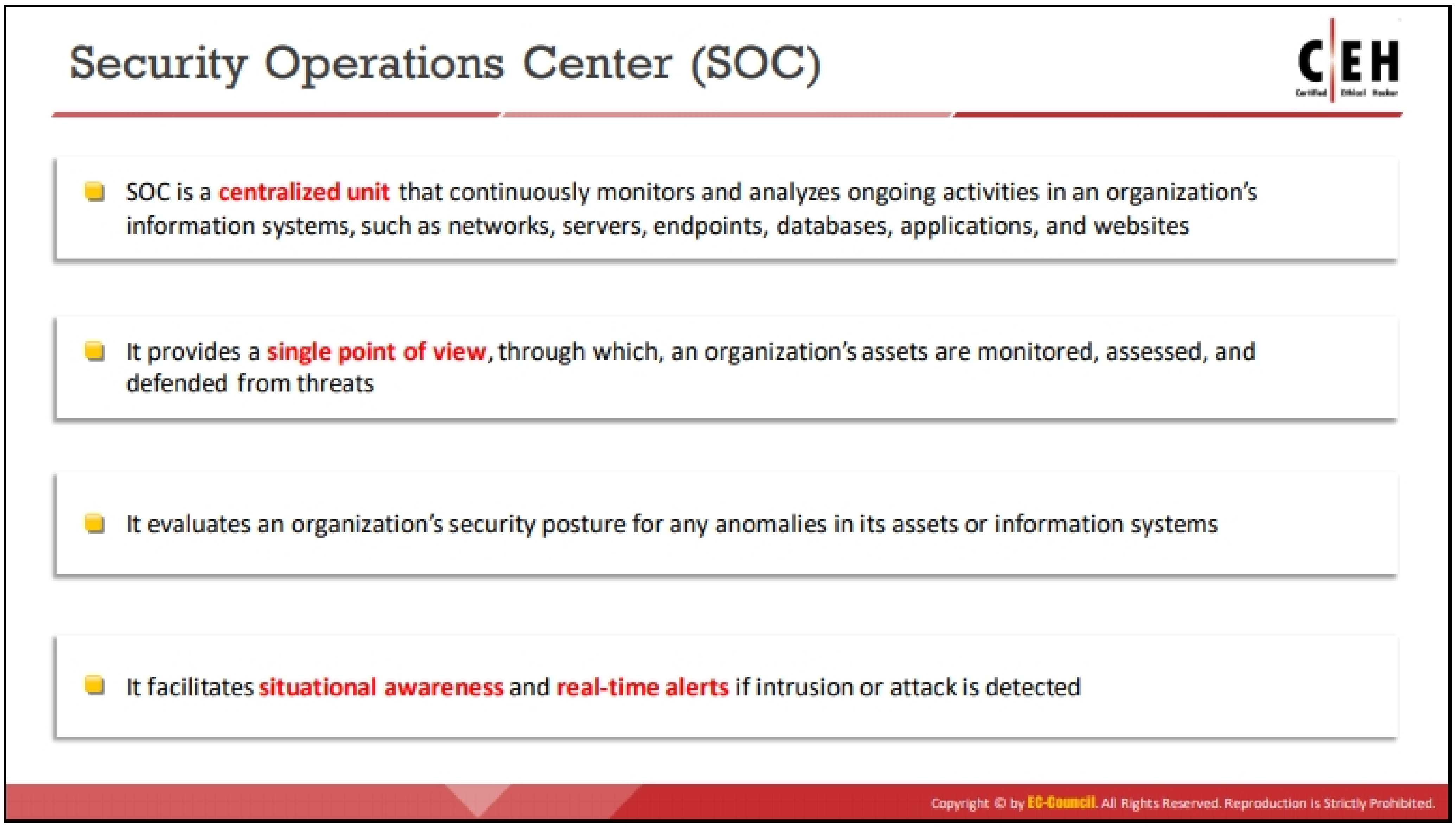
____

____



Security Operations

- The **continuous operational practice** for maintaining and managing a secure IT environment through the implementation and execution of certain services and processes
- The **predefined set of processes** and **services** that are to be followed during the daily security operation tasks, which are based on the organization's security baselines
- In recent security operations, organizations incorporated the third aspect of security operation, known as situational awareness, along with two traditional aspects of security operations: security monitoring and security incident management
  - **Situational Awareness**: Threat intelligence can play a vital role in creating situation awareness, making informed security decisions, and shaping cyber defenses accordingly
  - **Security Monitoring**: Collecting, storing, and analyzing logs and data from different security devices to identify security incidents
  - **Security Incident Management**: Resolving security incidents with minimal adverse impact
- A dedicated unit, known as **Security Operation Center (SOC)**, is established by organizations to handle and manage their security operations

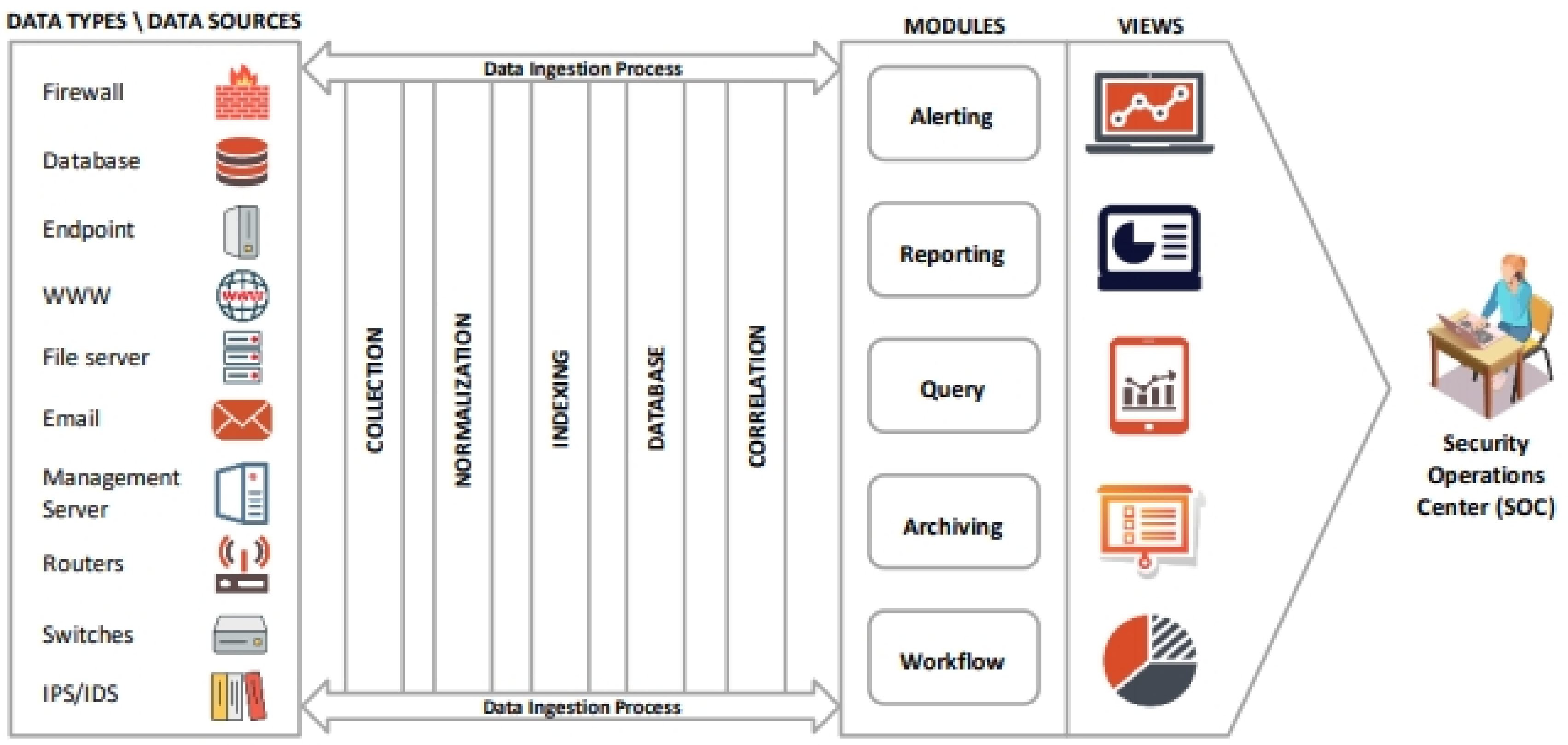


Security Operations Center (SOC)

- SOC is a **centralized unit** that continuously monitors and analyzes ongoing activities in an organization's information systems, such as networks, servers, endpoints, databases, applications, and websites
- It provides a **single point of view**, through which, an organization's assets are monitored, assessed, and defended from threats
- It evaluates an organization's security posture for any anomalies in its assets or information systems
- It facilitates **situational awareness** and **real-time alerts** if intrusion or attack is detected

Notes:

Security Operations Center (SOC) (Cont'd)



DATA TYPES \ DATA SOURCES

Firewall
Database
Endpoint
WWW
File server
Email
Management Server
Routers
Switches
IPS/IDS

Data Ingestion Process

COLLECTION
NORMALIZATION
INDEXING
DATABASE
CORRELATION

Data Ingestion Process

MODULES

Alerting
Reporting
Query
Archiving
Workflow

VIEWS

Security Operations Center (SOC)

SOC Operations

Log Collection

- Logs are collected from the various devices on a network that can have an impact on the security of the organization

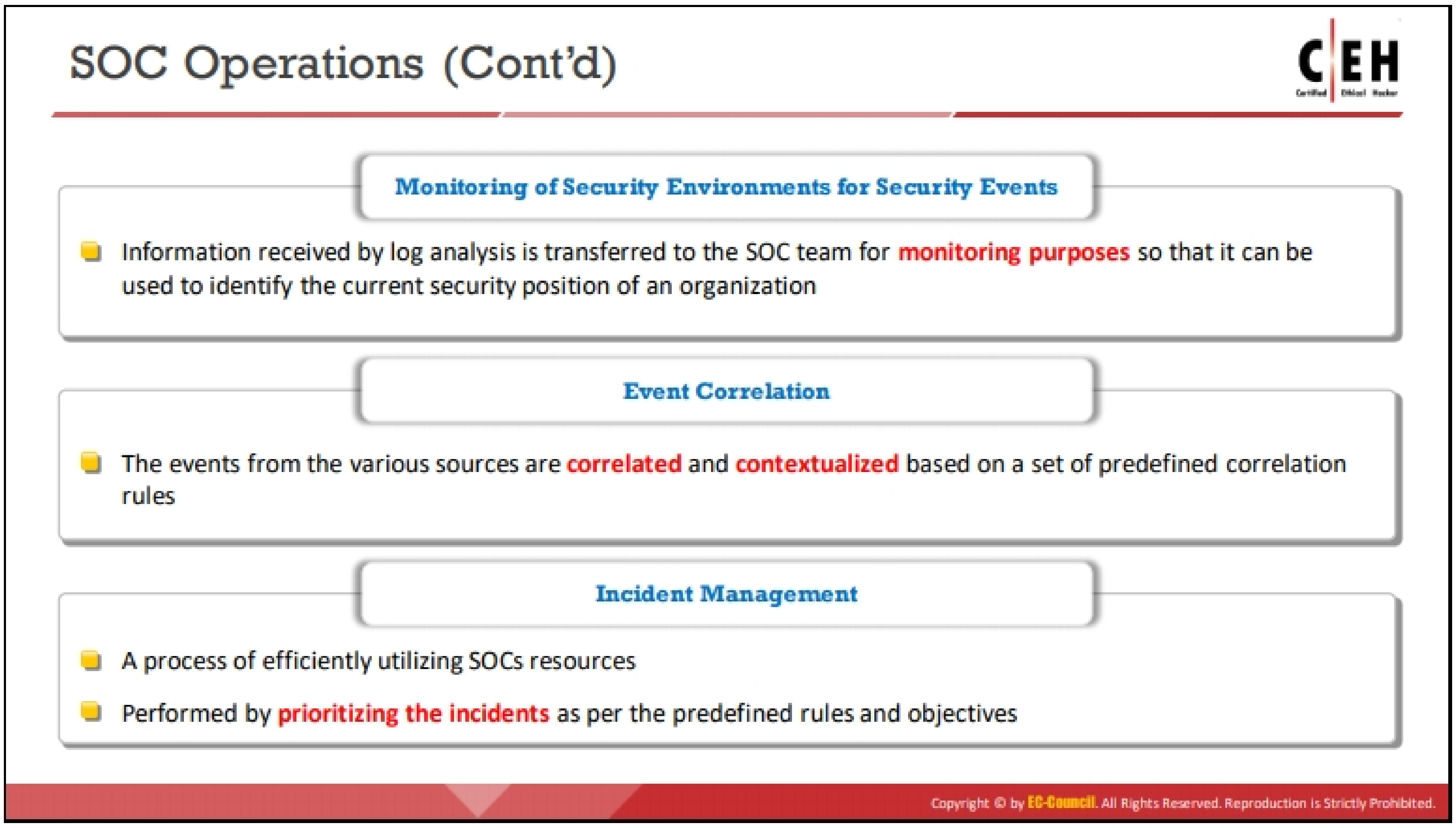
Log Retention and Archival

- Collected logs are **recovered** and **stored centrally**
- They can be used to perform **forensics** as well as **threat control** and **prevention**

Log Analysis

- Logs are analyzed through SOCs technology to extract important information such as relevant **metrics**, from the raw data

Notes: ____



SOC Operations (Cont'd)

Monitoring of Security Environments for Security Events

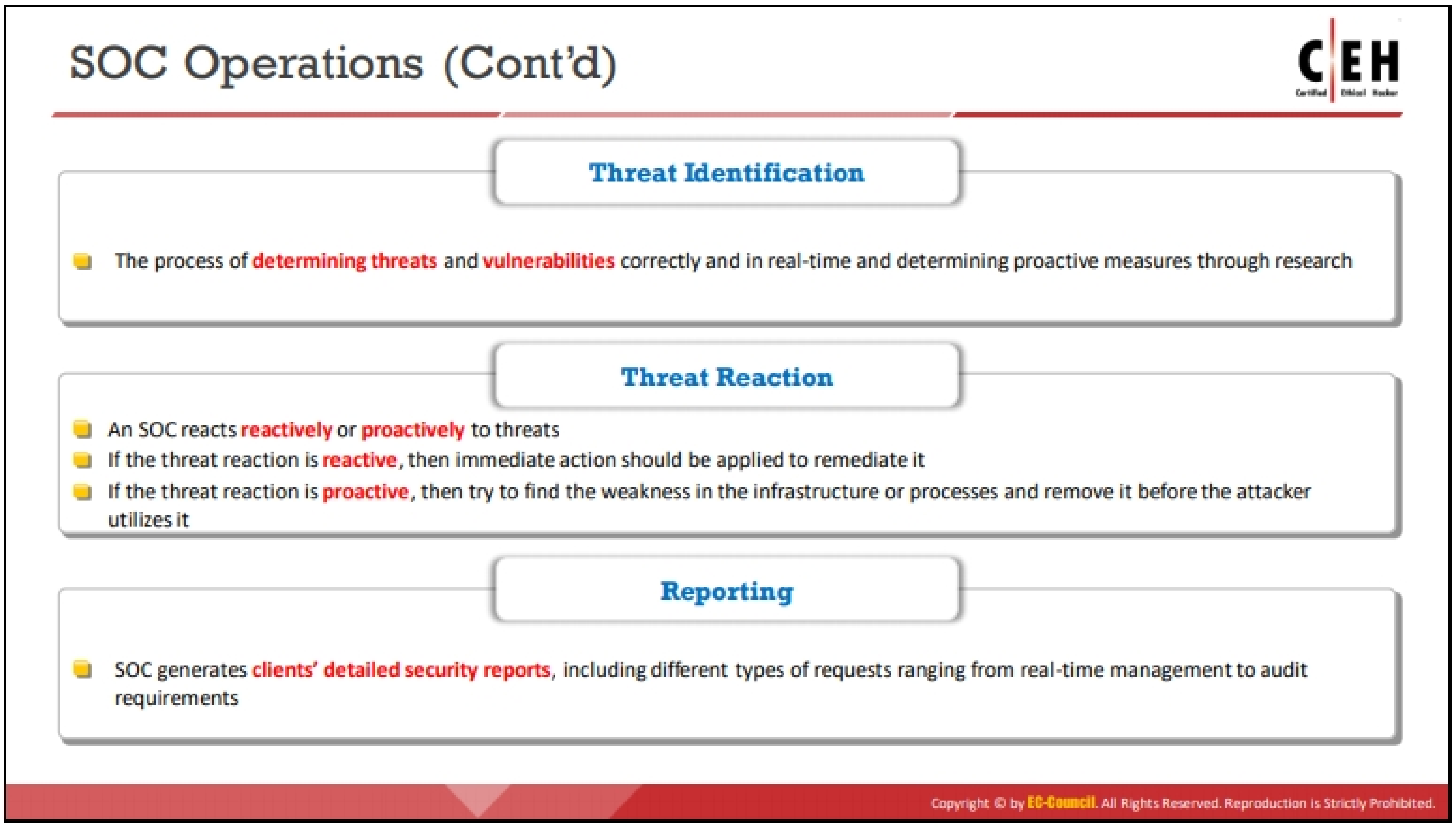
- Information received by log analysis is transferred to the SOC team for **monitoring purposes** so that it can be used to identify the current security position of an organization

Event Correlation

- The events from the various sources are **correlated** and **contextualized** based on a set of predefined correlation rules

Incident Management

- A process of efficiently utilizing SOCs resources
- Performed by **prioritizing the incidents** as per the predefined rules and objectives



SOC Operations (Cont'd)

Threat Identification

- The process of **determining threats** and **vulnerabilities** correctly and in real-time and determining proactive measures through research

Threat Reaction

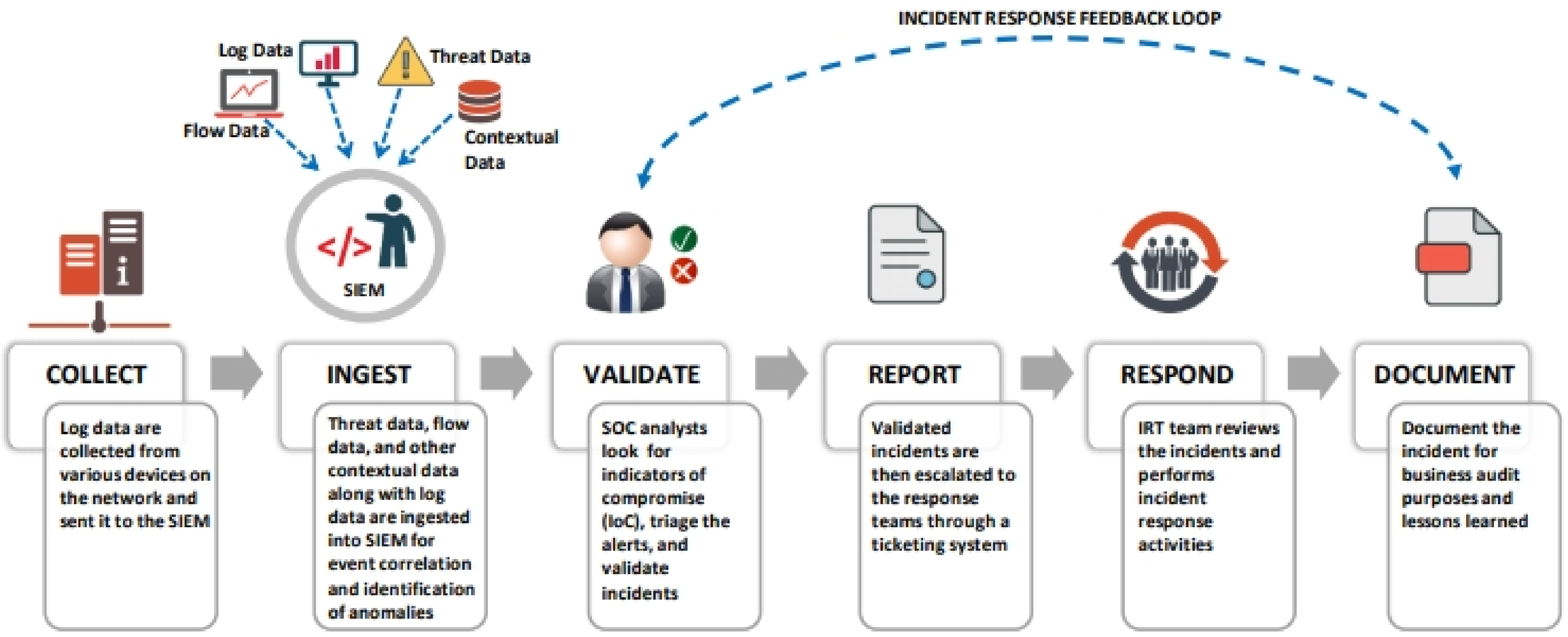
- An SOC reacts **reactively** or **proactively** to threats
- If the threat reaction is **reactive**, then immediate action should be applied to remediate it
- If the threat reaction is **proactive**, then try to find the weakness in the infrastructure or processes and remove it before the attacker utilizes it

Reporting

- SOC generates **clients' detailed security reports**, including different types of requests ranging from real-time management to audit requirements

Notes:

SOC Workflow



COLLECT

Log data are collected from various devices on the network and sent it to the SIEM

INGEST

Threat data, flow data, and other contextual data along with log data are ingested into SIEM for event correlation and identification of anomalies

VALIDATE

SOC analysts look for indicators of compromise (IoC), triage the alerts, and validate incidents

REPORT

Validated incidents are then escalated to the response teams through a ticketing system

RESPOND

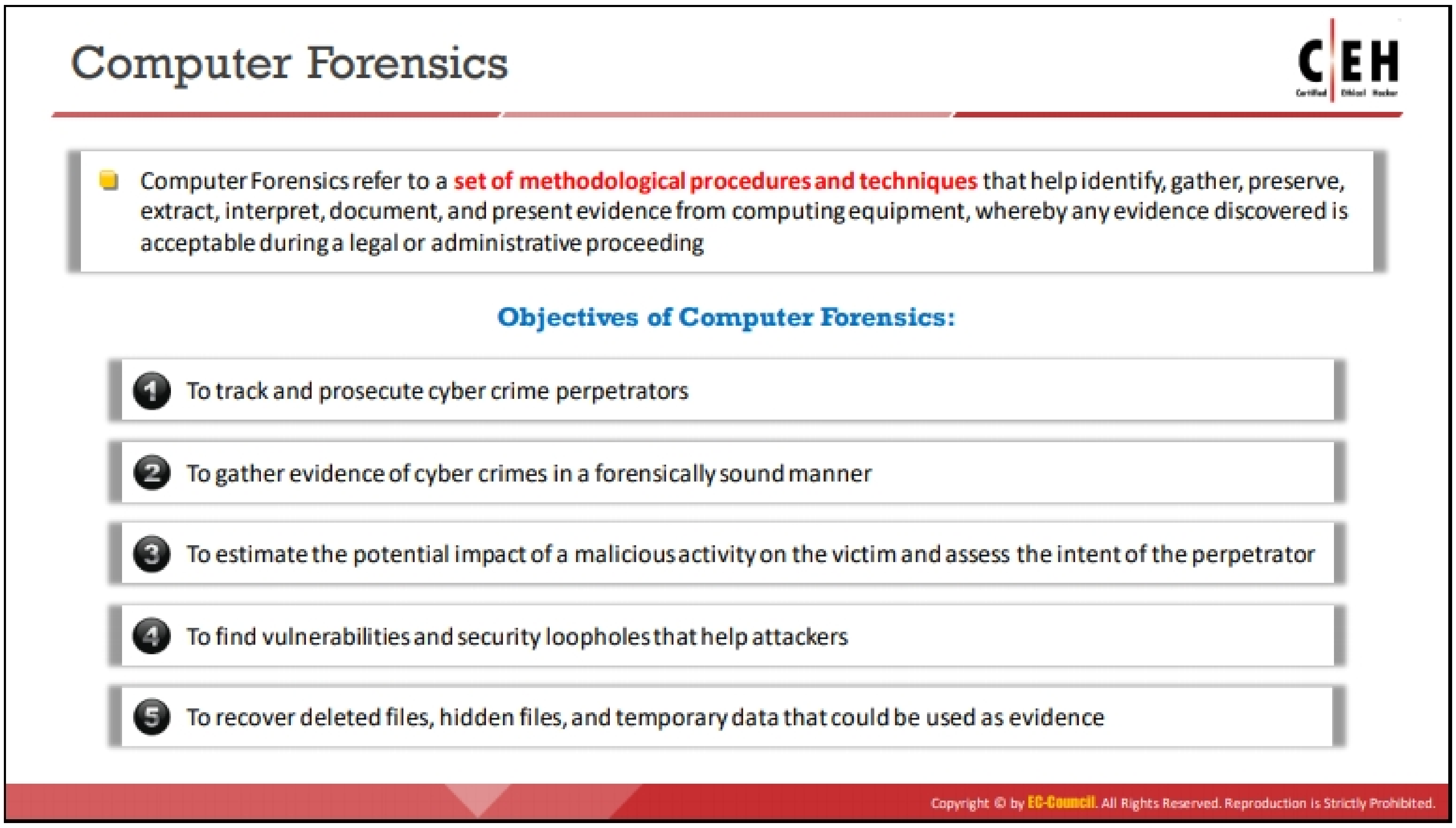
IRT team reviews the incidents and performs incident response activities

DOCUMENT

Document the incident for business audit purposes and lessons learned

Forensic Investigation

Notes: ____________________

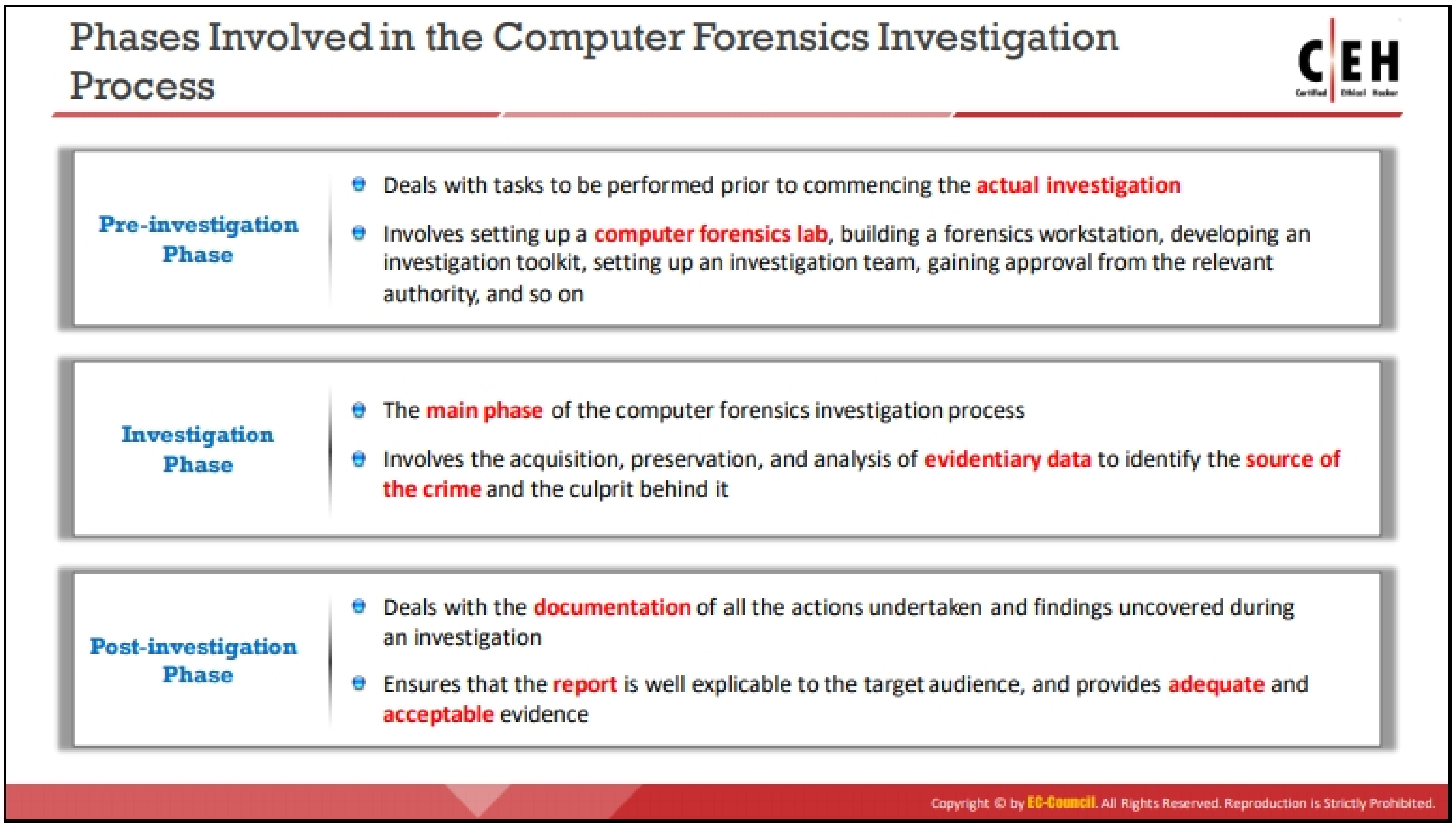


Computer Forensics

- Computer Forensics refer to a set of methodological procedures and techniques that help identify, gather, preserve, extract, interpret, document, and present evidence from computing equipment, whereby any evidence discovered is acceptable during a legal or administrative proceeding

Objectives of Computer Forensics:

1. To track and prosecute cyber crime perpetrators
2. To gather evidence of cyber crimes in a forensically sound manner
3. To estimate the potential impact of a malicious activity on the victim and assess the intent of the perpetrator
4. To find vulnerabilities and security loopholes that help attackers
5. To recover deleted files, hidden files, and temporary data that could be used as evidence



Phases Involved in the Computer Forensics Investigation Process

Pre-investigation Phase

- Deals with tasks to be performed prior to commencing the actual investigation
- Involves setting up a computer forensics lab, building a forensics workstation, developing an investigation toolkit, setting up an investigation team, gaining approval from the relevant authority, and so on

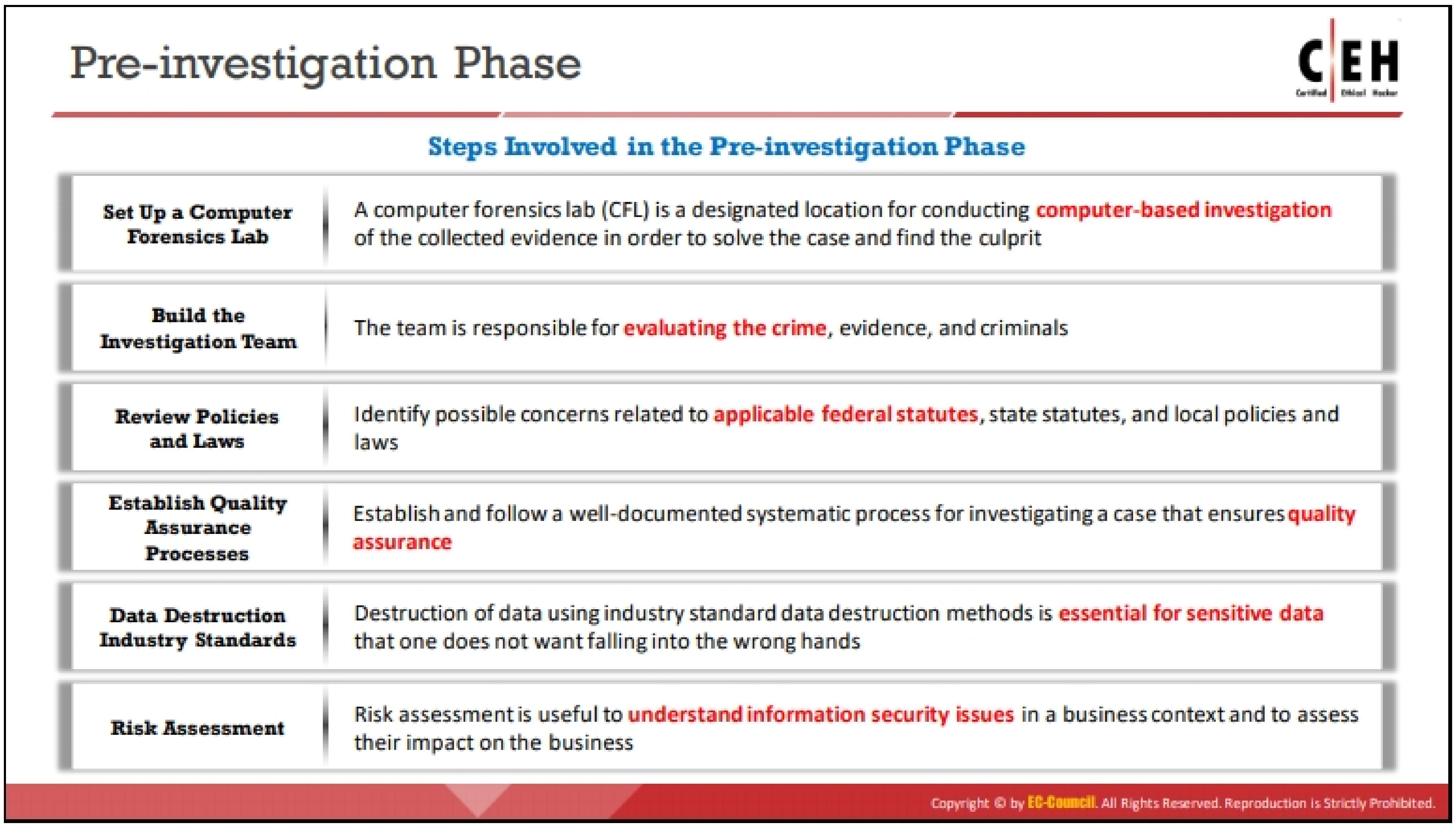
Investigation Phase

- The main phase of the computer forensics investigation process
- Involves the acquisition, preservation, and analysis of evidentiary data to identify the source of the crime and the culprit behind it

Post-investigation Phase

- Deals with the documentation of all the actions undertaken and findings uncovered during an investigation
- Ensures that the report is well explicable to the target audience, and provides adequate and acceptable evidence

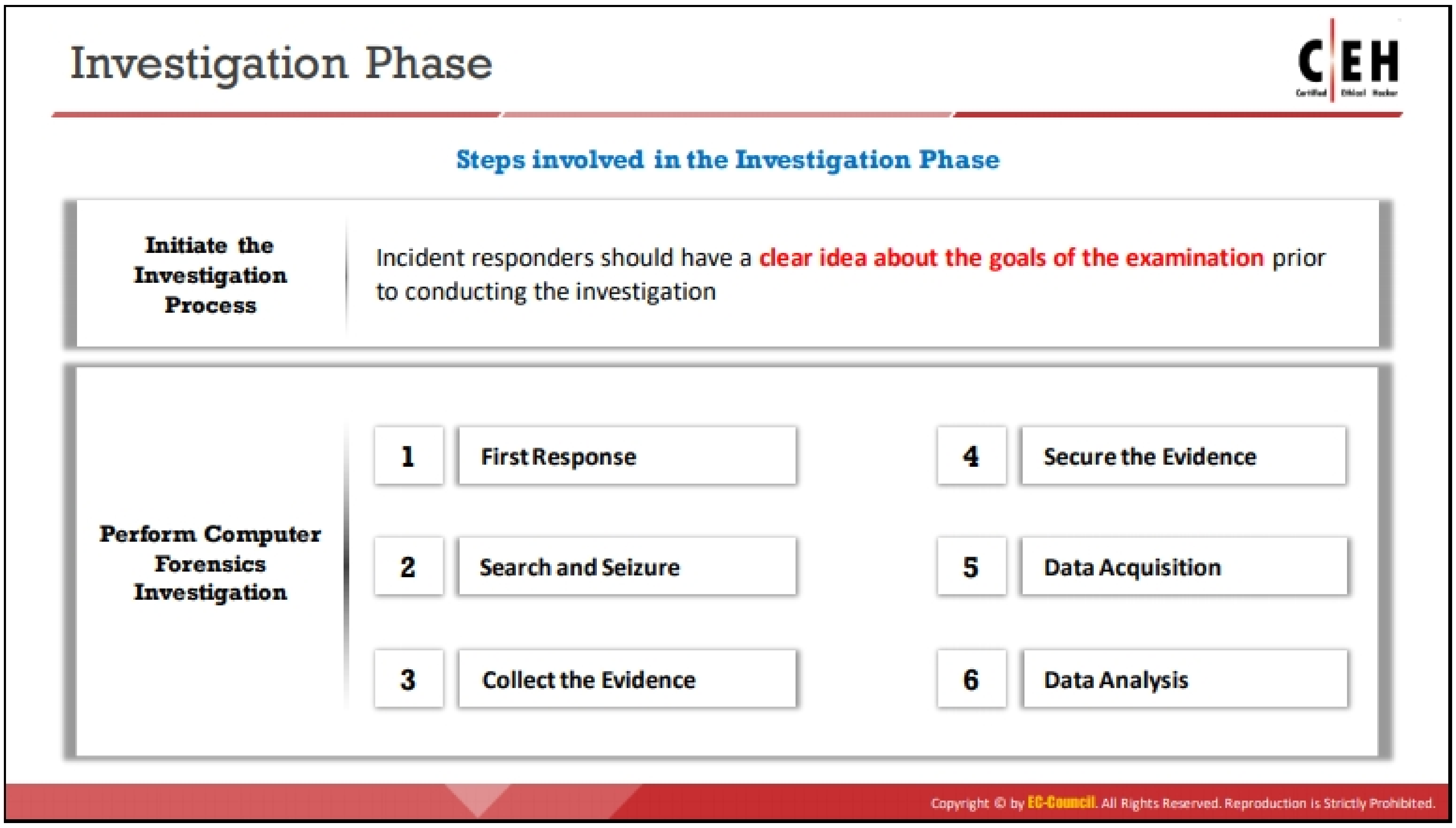
Notes: ____



Pre-investigation Phase

Steps Involved in the Pre-investigation Phase

Set Up a Computer Forensics Lab	A computer forensics lab (CFL) is a designated location for conducting **computer-based investigation** of the collected evidence in order to solve the case and find the culprit
Build the Investigation Team	The team is responsible for **evaluating the crime**, evidence, and criminals
Review Policies and Laws	Identify possible concerns related to **applicable federal statutes**, state statutes, and local policies and laws
Establish Quality Assurance Processes	Establish and follow a well-documented systematic process for investigating a case that ensures **quality assurance**
Data Destruction Industry Standards	Destruction of data using industry standard data destruction methods is **essential for sensitive data** that one does not want falling into the wrong hands
Risk Assessment	Risk assessment is useful to **understand information security issues** in a business context and to assess their impact on the business



Investigation Phase

Steps involved in the Investigation Phase

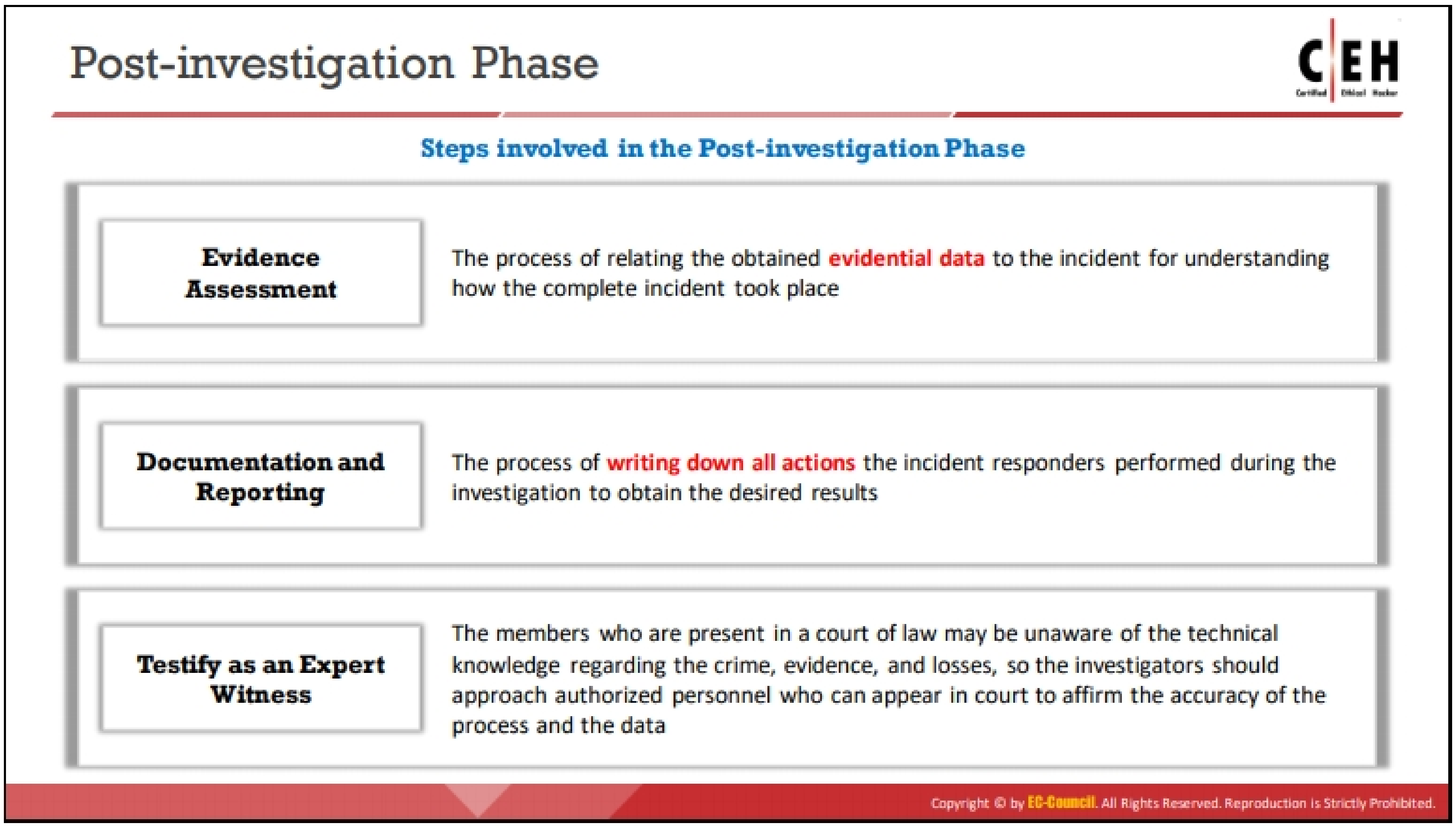
Initiate the Investigation Process

Incident responders should have a **clear idea about the goals of the examination** prior to conducting the investigation

Perform Computer Forensics Investigation

1. First Response
2. Search and Seizure
3. Collect the Evidence
4. Secure the Evidence
5. Data Acquisition
6. Data Analysis

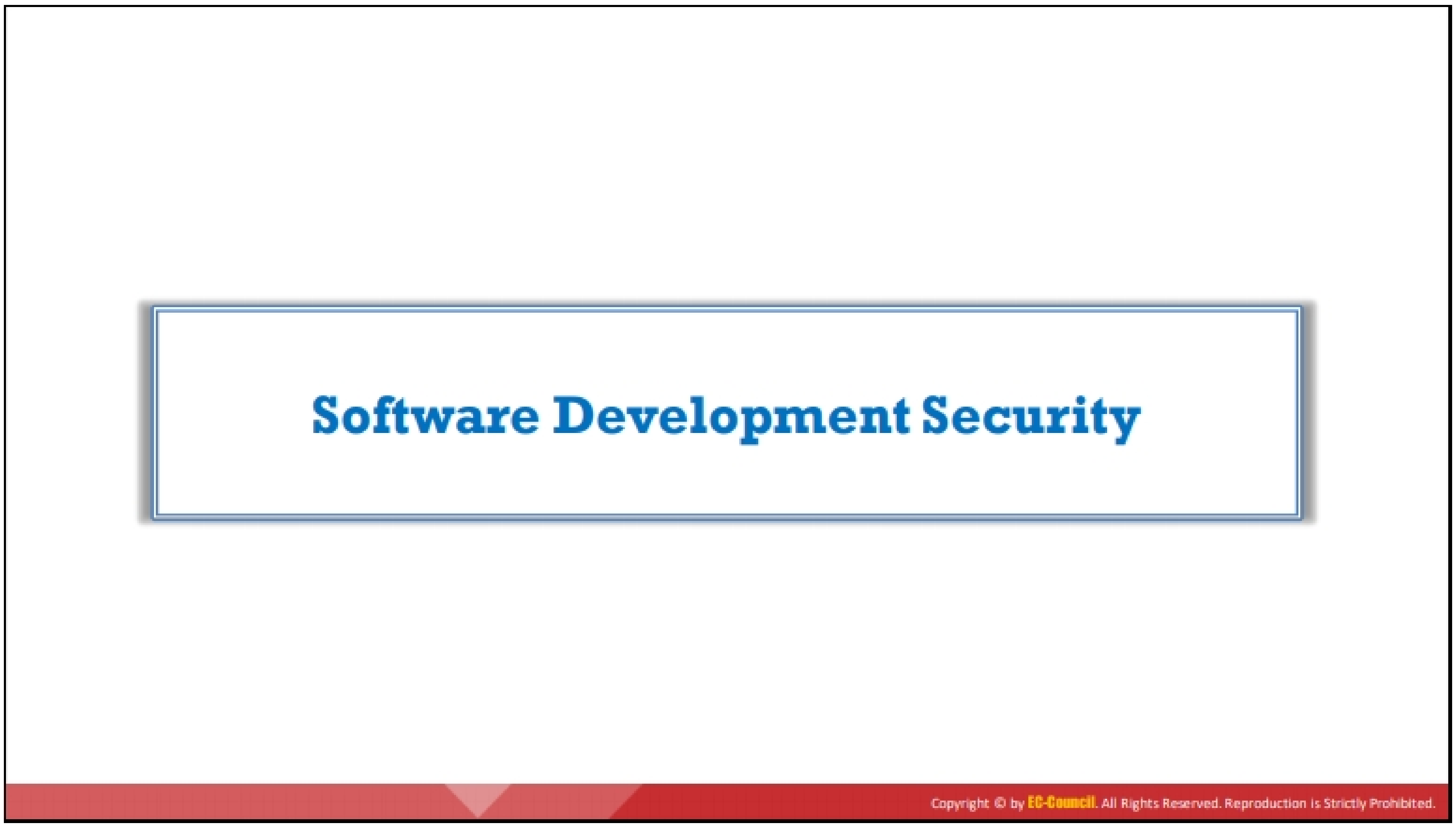
Notes: ____



Post-investigation Phase

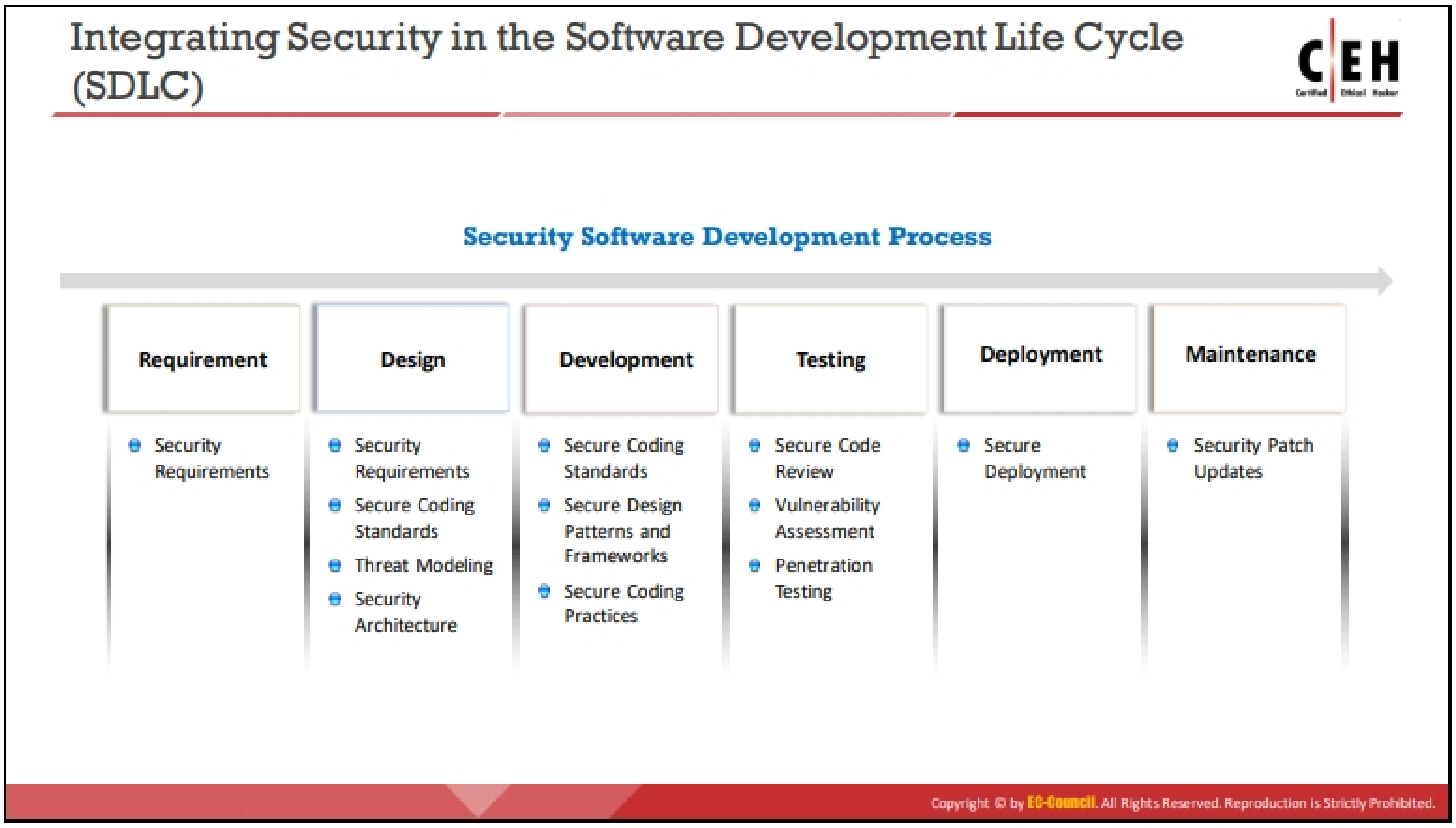
Steps involved in the Post-investigation Phase

Evidence Assessment	The process of relating the obtained **evidential data** to the incident for understanding how the complete incident took place
Documentation and Reporting	The process of **writing down all actions** the incident responders performed during the investigation to obtain the desired results
Testify as an Expert Witness	The members who are present in a court of law may be unaware of the technical knowledge regarding the crime, evidence, and losses, so the investigators should approach authorized personnel who can appear in court to affirm the accuracy of the process and the data



Software Development Security

Notes: ____



Integrating Security in the Software Development Life Cycle (SDLC)

Security Software Development Process

Requirement
- Security Requirements

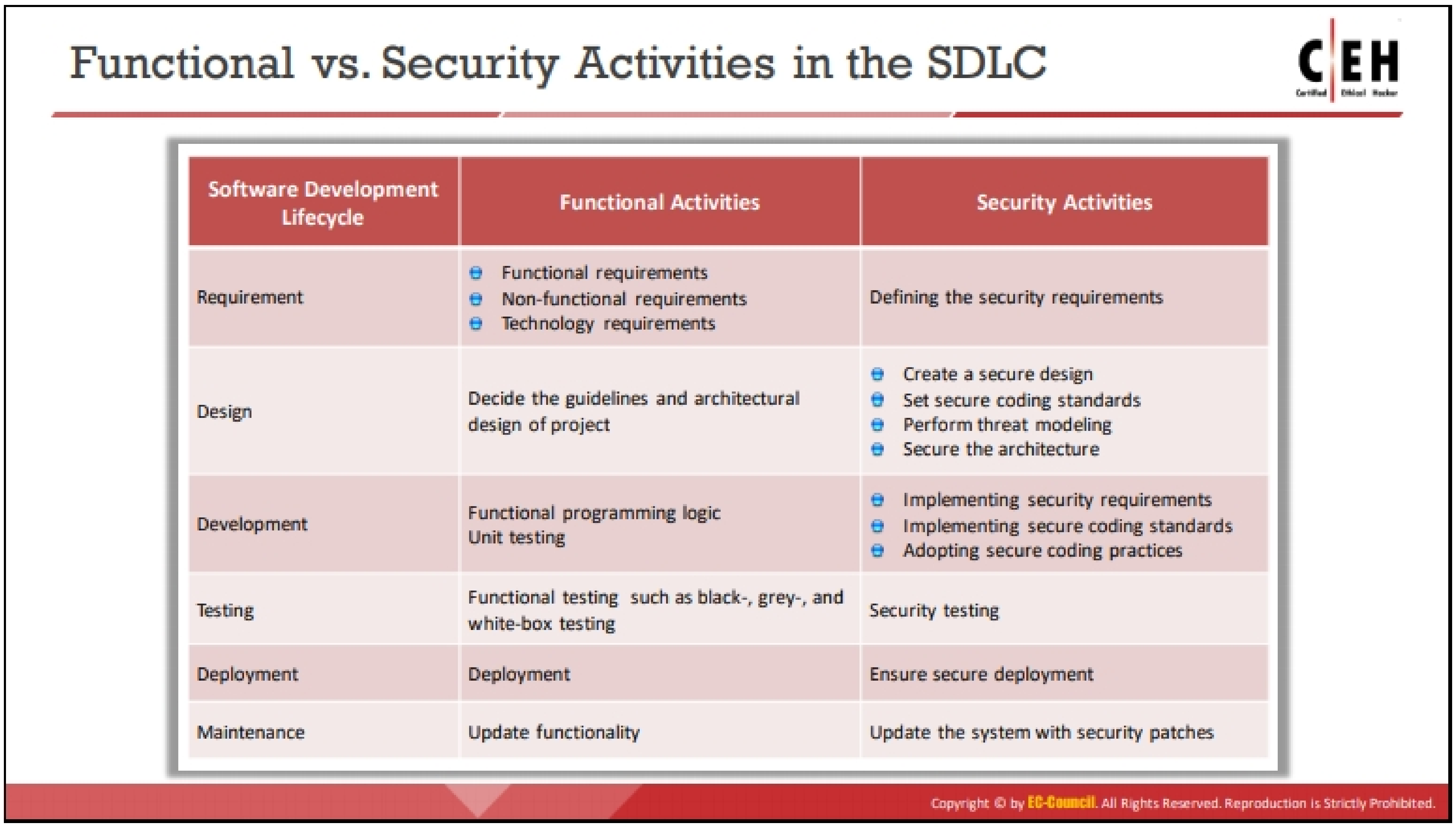
Design
- Security Requirements
- Secure Coding Standards
- Threat Modeling
- Security Architecture

Development
- Secure Coding Standards
- Secure Design Patterns and Frameworks
- Secure Coding Practices

Testing
- Secure Code Review
- Vulnerability Assessment
- Penetration Testing

Deployment
- Secure Deployment

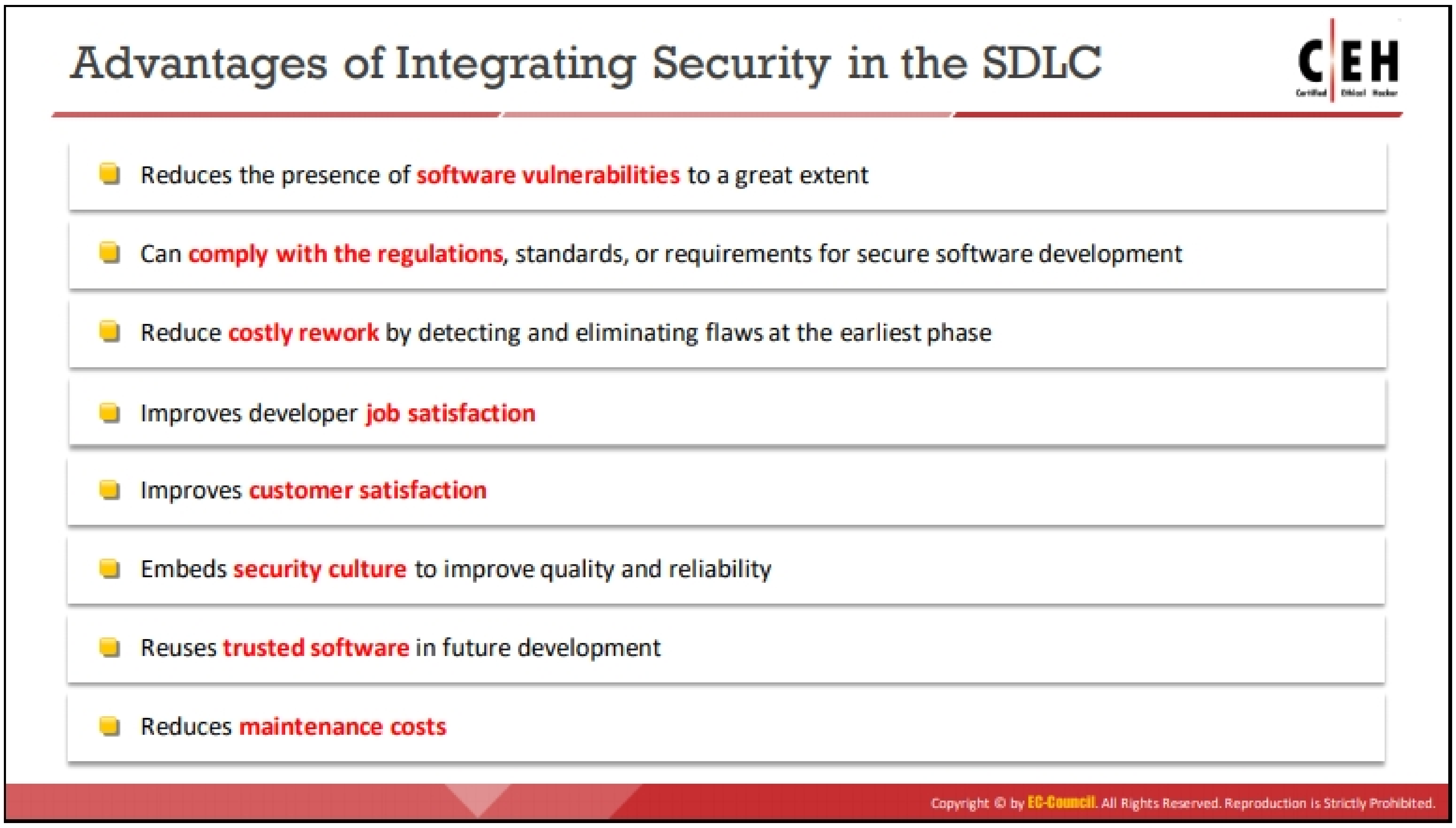
Maintenance
- Security Patch Updates



Functional vs. Security Activities in the SDLC

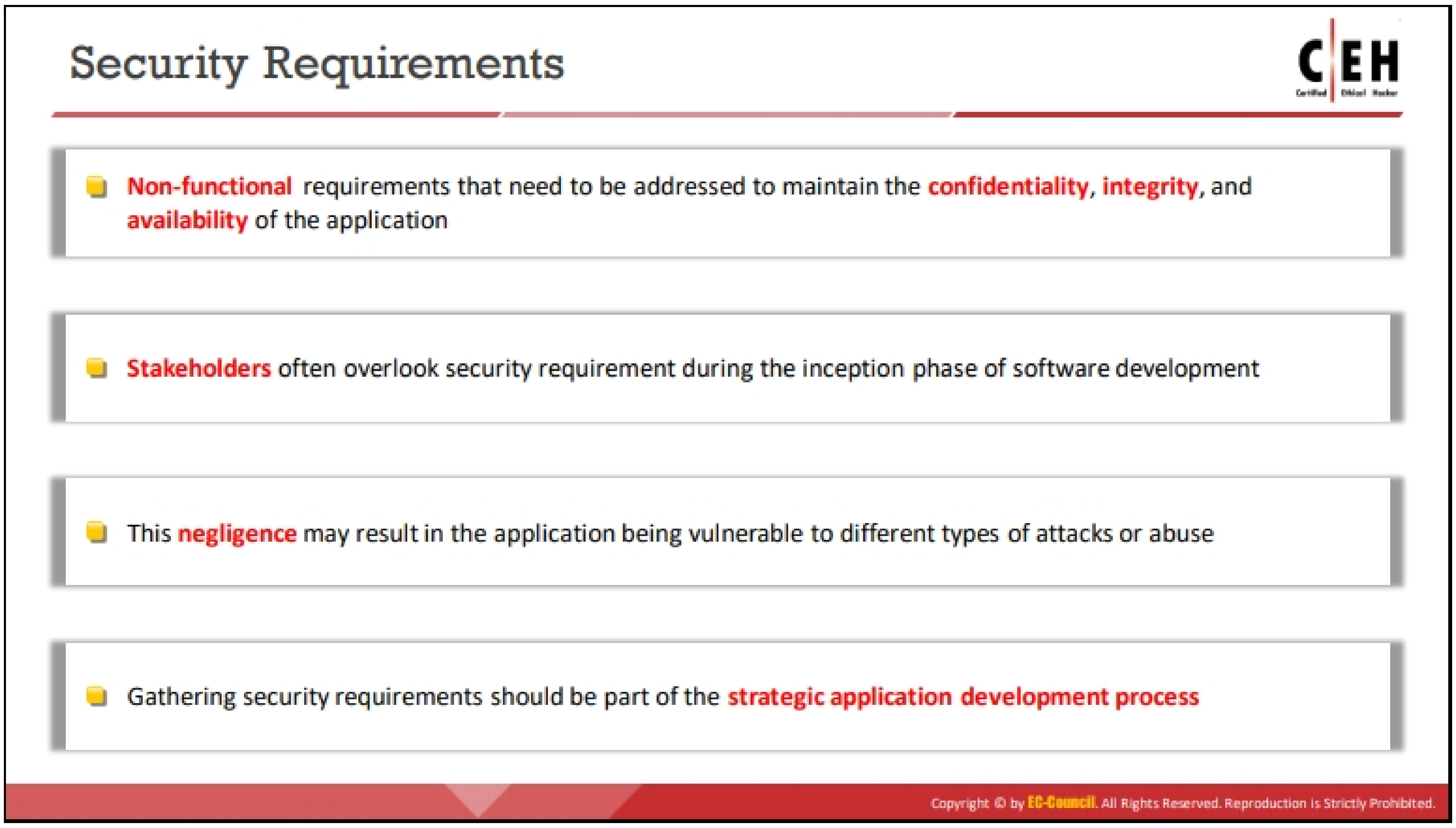
Software Development Lifecycle	Functional Activities	Security Activities
Requirement	- Functional requirements - Non-functional requirements - Technology requirements	Defining the security requirements
Design	Decide the guidelines and architectural design of project	- Create a secure design - Set secure coding standards - Perform threat modeling - Secure the architecture
Development	Functional programming logic Unit testing	- Implementing security requirements - Implementing secure coding standards - Adopting secure coding practices
Testing	Functional testing such as black-, grey-, and white-box testing	Security testing
Deployment	Deployment	Ensure secure deployment
Maintenance	Update functionality	Update the system with security patches

Notes: ____



Advantages of Integrating Security in the SDLC

- Reduces the presence of **software vulnerabilities** to a great extent
- Can **comply with the regulations**, standards, or requirements for secure software development
- Reduce **costly rework** by detecting and eliminating flaws at the earliest phase
- Improves developer **job satisfaction**
- Improves **customer satisfaction**
- Embeds **security culture** to improve quality and reliability
- Reuses **trusted software** in future development
- Reduces **maintenance costs**



Security Requirements

- **Non-functional** requirements that need to be addressed to maintain the **confidentiality**, **integrity**, and **availability** of the application
- **Stakeholders** often overlook security requirement during the inception phase of software development
- This **negligence** may result in the application being vulnerable to different types of attacks or abuse
- Gathering security requirements should be part of the **strategic application development process**

Notes: ____

____

____

____

____

____

Gathering Security Requirements

① Eliciting software security requirements takes different approaches

② Security Requirements should be enumerated separately from the functional requirement so that they can be separately reviewed and tested

③ Mixing the security requirement with the functional requirement can make the security requirement gathering process more complicated and less accurate

Why We Need Different Approaches for Security Requirement Gathering

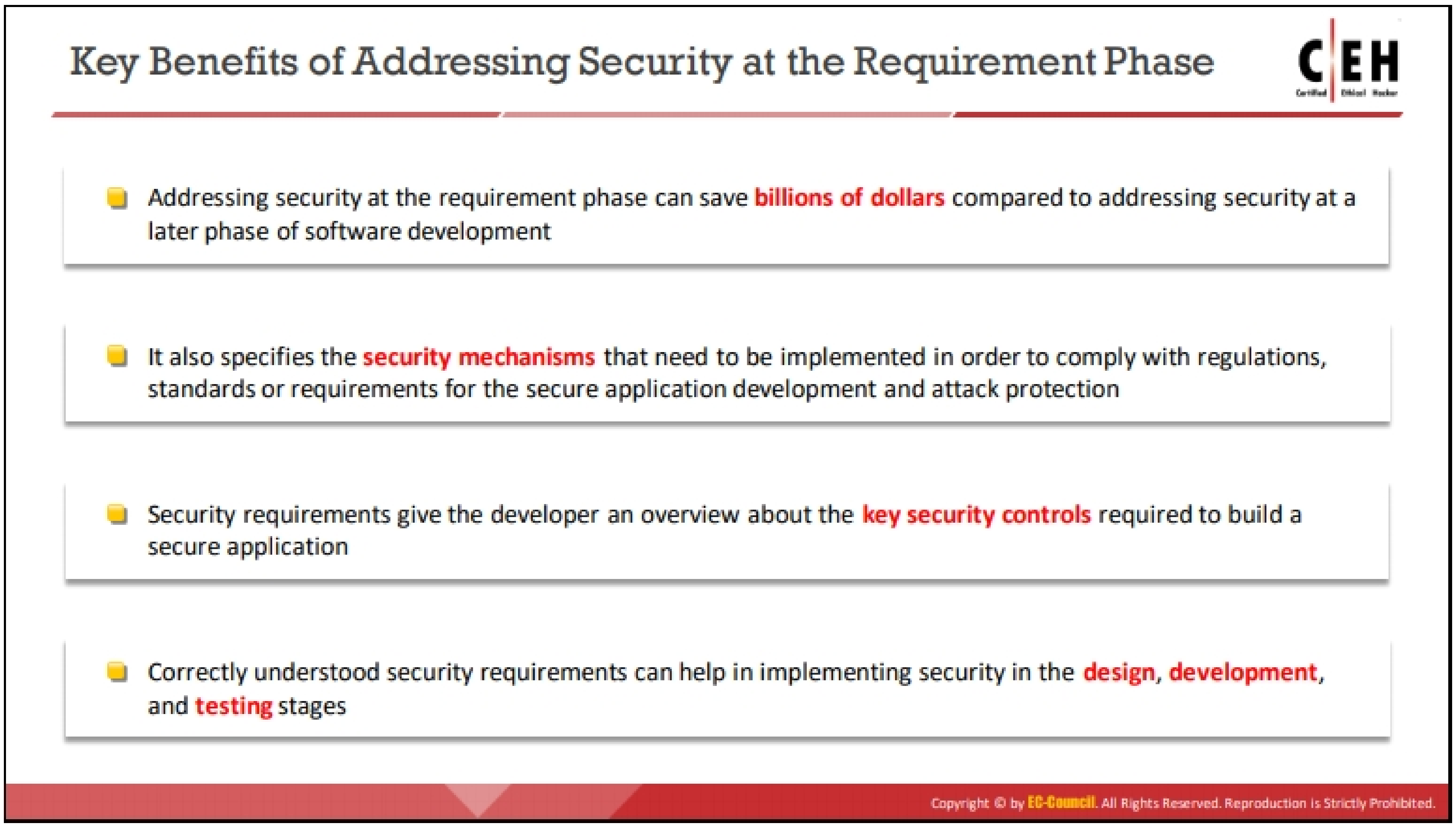
① Functional requirements are positive requirements specifying what the software should do

② Security requirements are negative requirements specifying what the software should not do

③ It is the natural tendency of people to be clear about what they want but to find it difficult to understand things they don't want

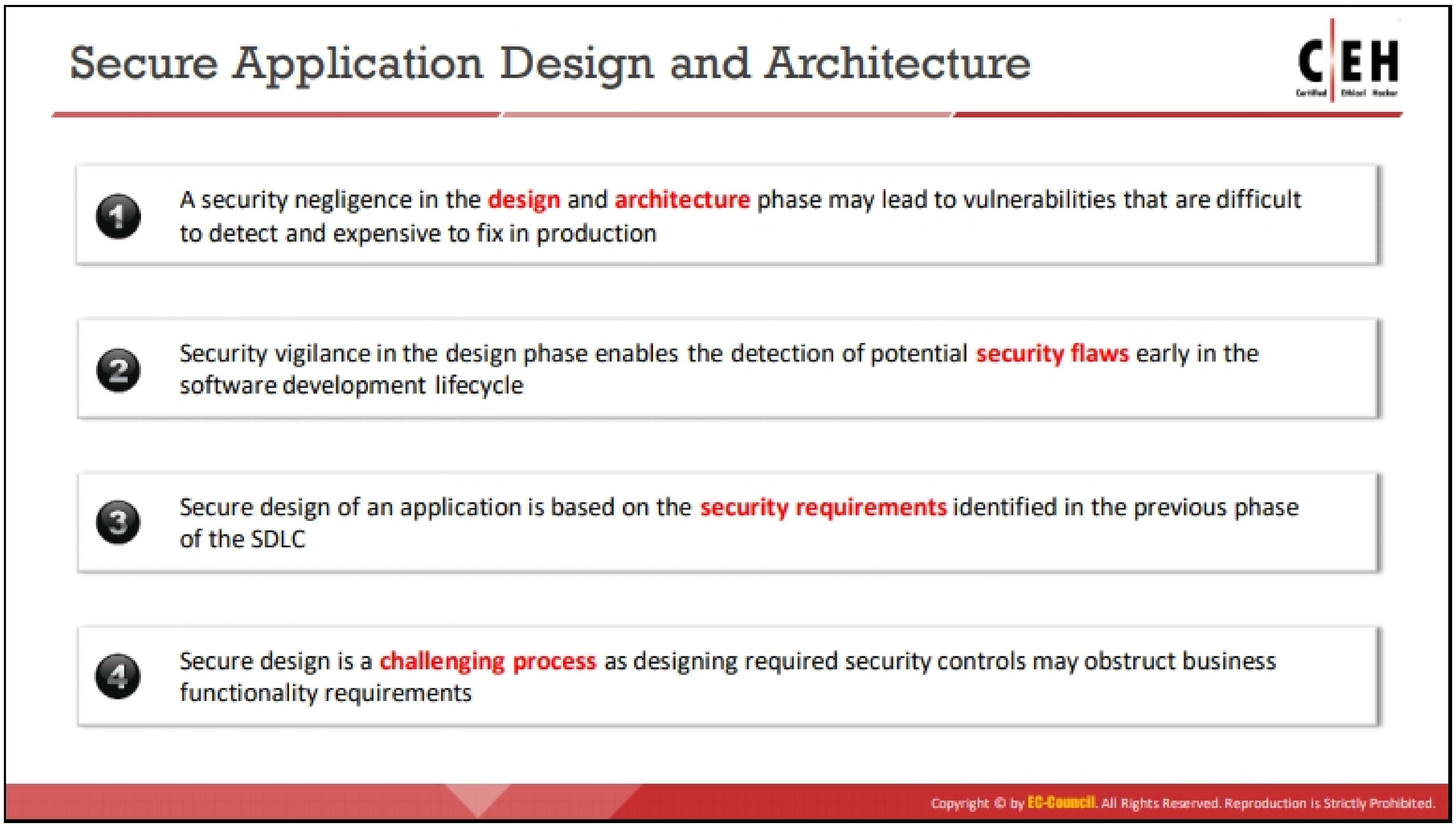
④ Software needs to be viewed in a more negative, critical, and destructive way to reveal its non-intended use and its associated security requirements

Notes: ____



Key Benefits of Addressing Security at the Requirement Phase

- Addressing security at the requirement phase can save **billions of dollars** compared to addressing security at a later phase of software development
- It also specifies the **security mechanisms** that need to be implemented in order to comply with regulations, standards or requirements for the secure application development and attack protection
- Security requirements give the developer an overview about the **key security controls** required to build a secure application
- Correctly understood security requirements can help in implementing security in the **design**, **development**, and **testing** stages



Secure Application Design and Architecture

1. A security negligence in the **design** and **architecture** phase may lead to vulnerabilities that are difficult to detect and expensive to fix in production
2. Security vigilance in the design phase enables the detection of potential **security flaws** early in the software development lifecycle
3. Secure design of an application is based on the **security requirements** identified in the previous phase of the SDLC
4. Secure design is a **challenging process** as designing required security controls may obstruct business functionality requirements

Notes: ____

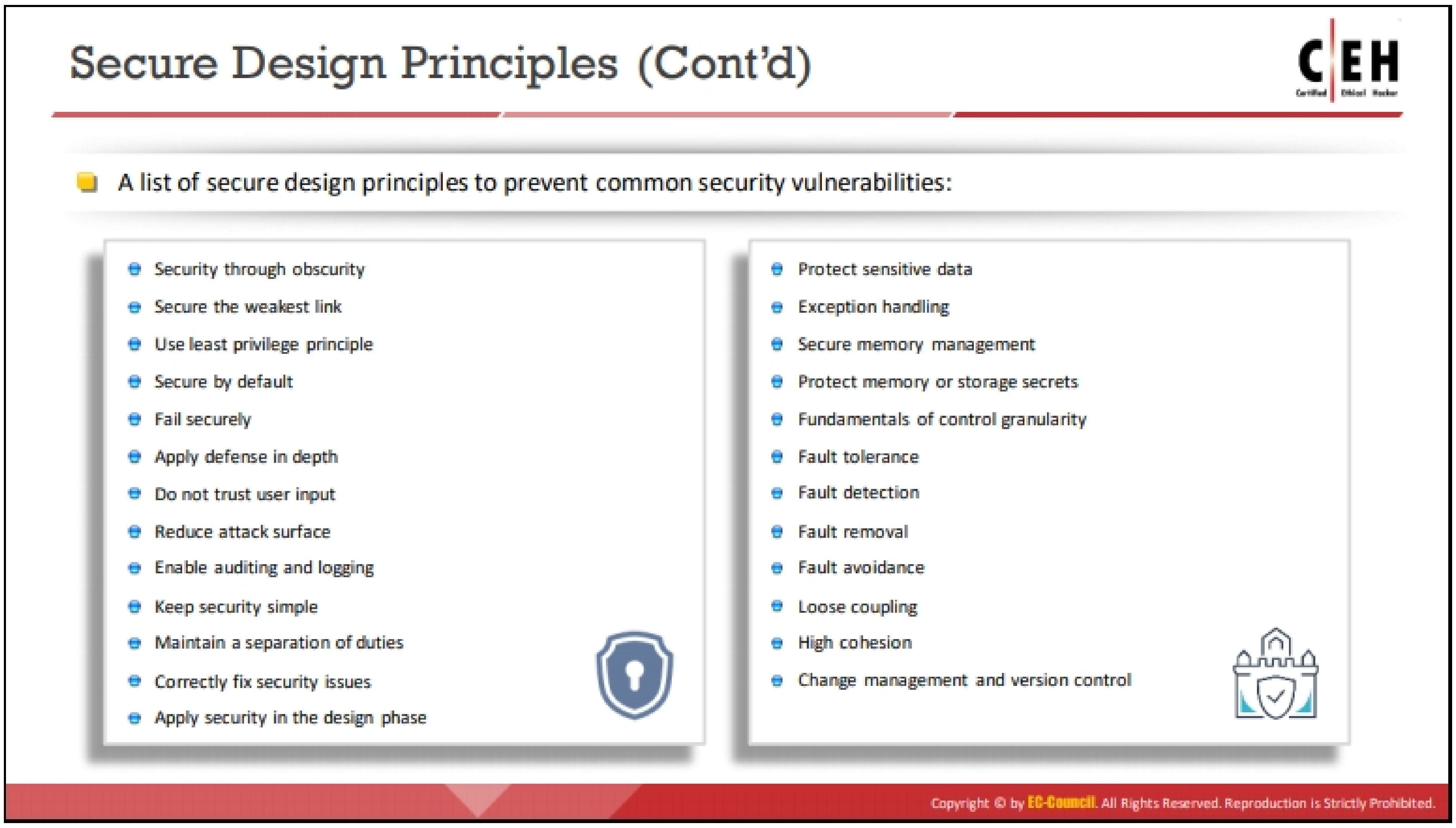
Goals of the Secure Design Process

- Identify the threats in sufficient enough detail for **developers** to understand and code accordingly to mitigate the associated risk
- Design the **architecture** in such a way that it mitigates as many threats as possible
- Enforce **secure design principles** that force developers to consider security while coding

Secure Design Principles

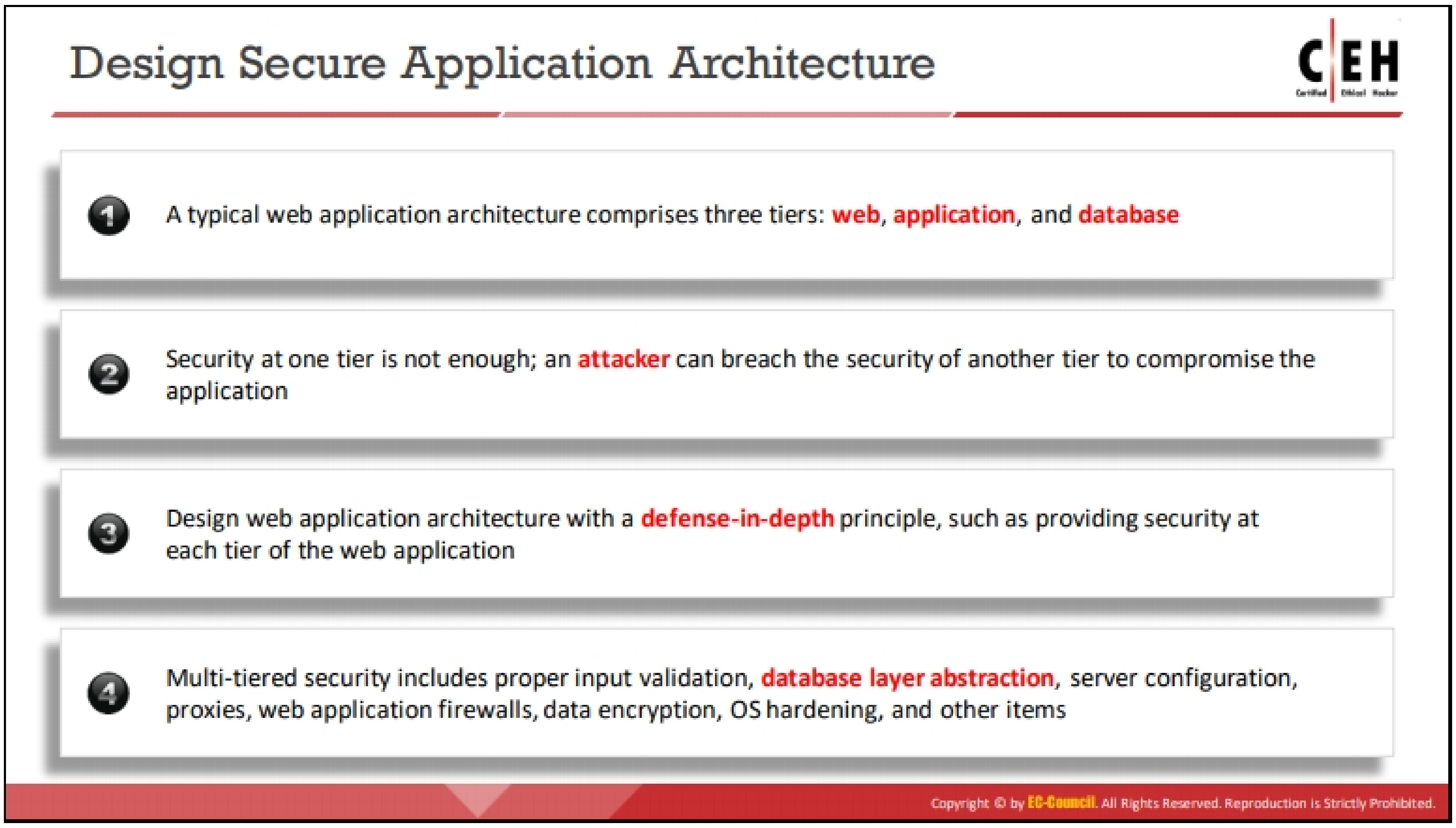
- Secure Design Principles are the **practices or guidelines** that should be enforced on the developers during the development phase
- They help in deriving **secure architectural decisions**
- They help to eliminate design and architecture **flaws** and mitigate common security vulnerabilities within the application

Notes: ____



Secure Design Principles (Cont'd)

- A list of secure design principles to prevent common security vulnerabilities:
  - Security through obscurity
  - Secure the weakest link
  - Use least privilege principle
  - Secure by default
  - Fail securely
  - Apply defense in depth
  - Do not trust user input
  - Reduce attack surface
  - Enable auditing and logging
  - Keep security simple
  - Maintain a separation of duties
  - Correctly fix security issues
  - Apply security in the design phase
  - Protect sensitive data
  - Exception handling
  - Secure memory management
  - Protect memory or storage secrets
  - Fundamentals of control granularity
  - Fault tolerance
  - Fault detection
  - Fault removal
  - Fault avoidance
  - Loose coupling
  - High cohesion
  - Change management and version control



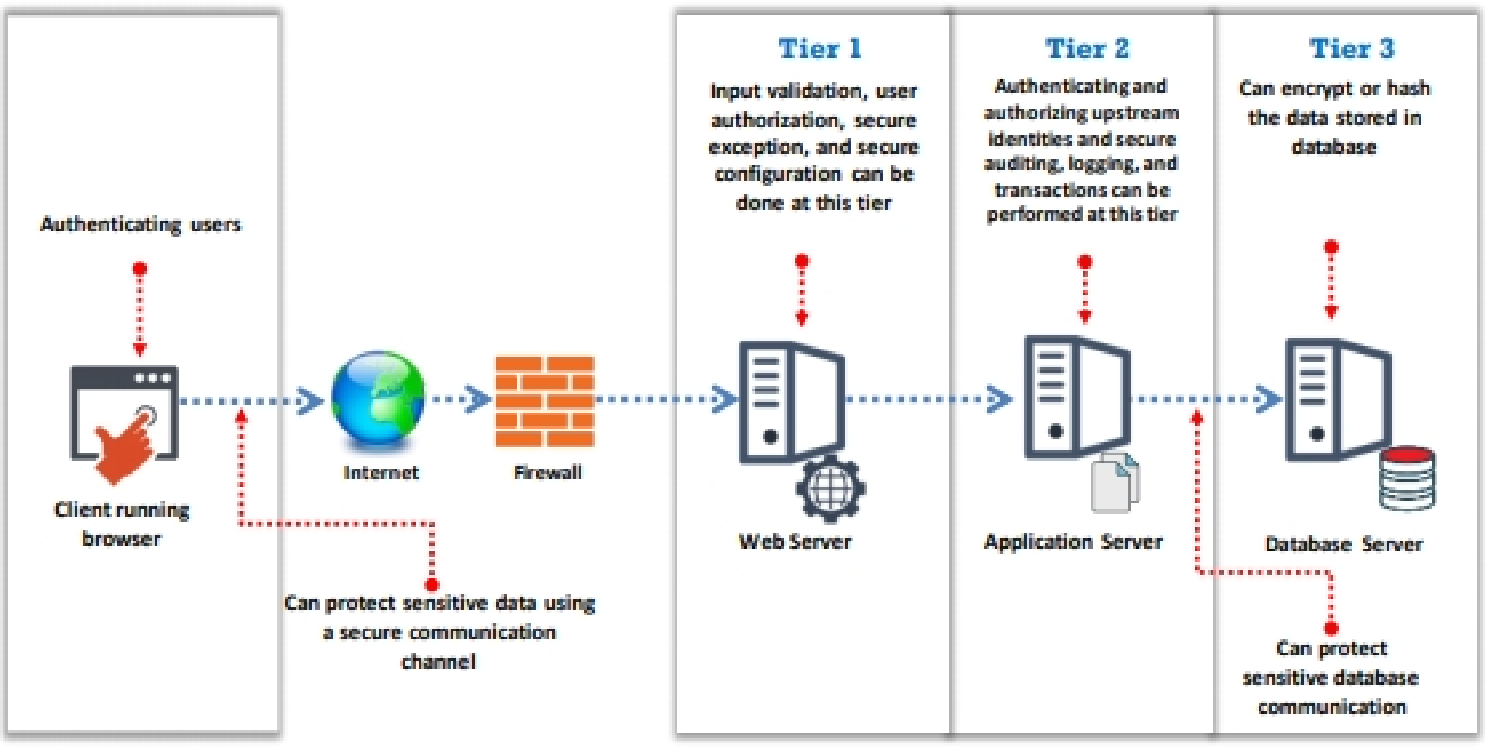
Design Secure Application Architecture

1. A typical web application architecture comprises three tiers: **web**, **application**, and **database**
2. Security at one tier is not enough; an **attacker** can breach the security of another tier to compromise the application
3. Design web application architecture with a **defense-in-depth** principle, such as providing security at each tier of the web application
4. Multi-tiered security includes proper input validation, **database layer abstraction**, server configuration, proxies, web application firewalls, data encryption, OS hardening, and other items

Notes:

Design Secure Application Architecture (Cont'd)

- Applying multiple layer security in application architecture design makes an application robust and secure


Authenticating users
Client running browser
Internet
Firewall
Can protect sensitive data using a secure communication channel
Tier 1
Input validation, user authorization, secure exception, and secure configuration can be done at this tier
Web Server
Tier 2
Authenticating and authorizing upstream identities and secure auditing, logging, and transactions can be performed at this tier
Application Server
Tier 3
Can encrypt or hash the data stored in database
Database Server
Can protect sensitive database communication

Security Governance Principles

Notes: ____

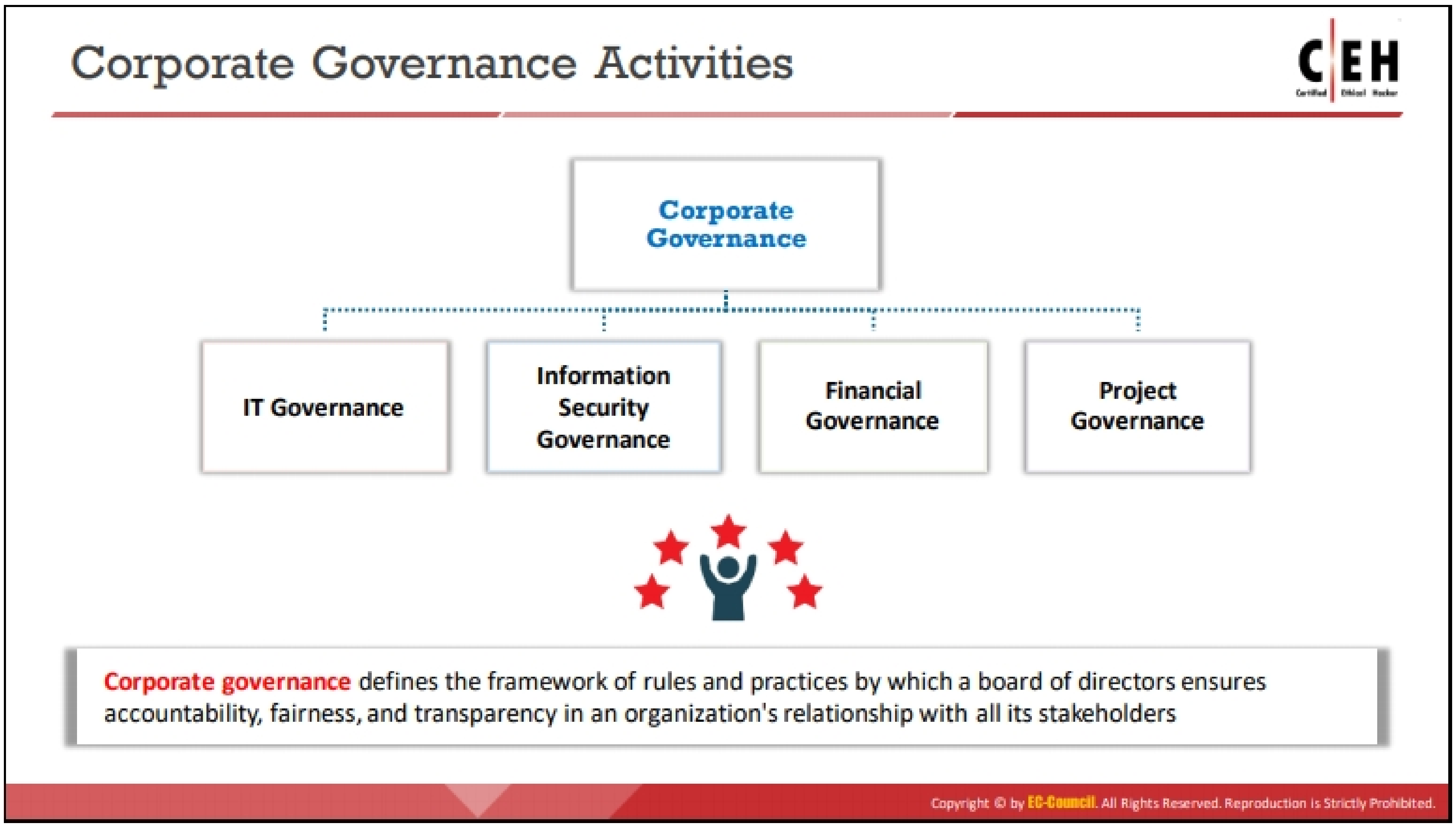
____

____

____

____

____

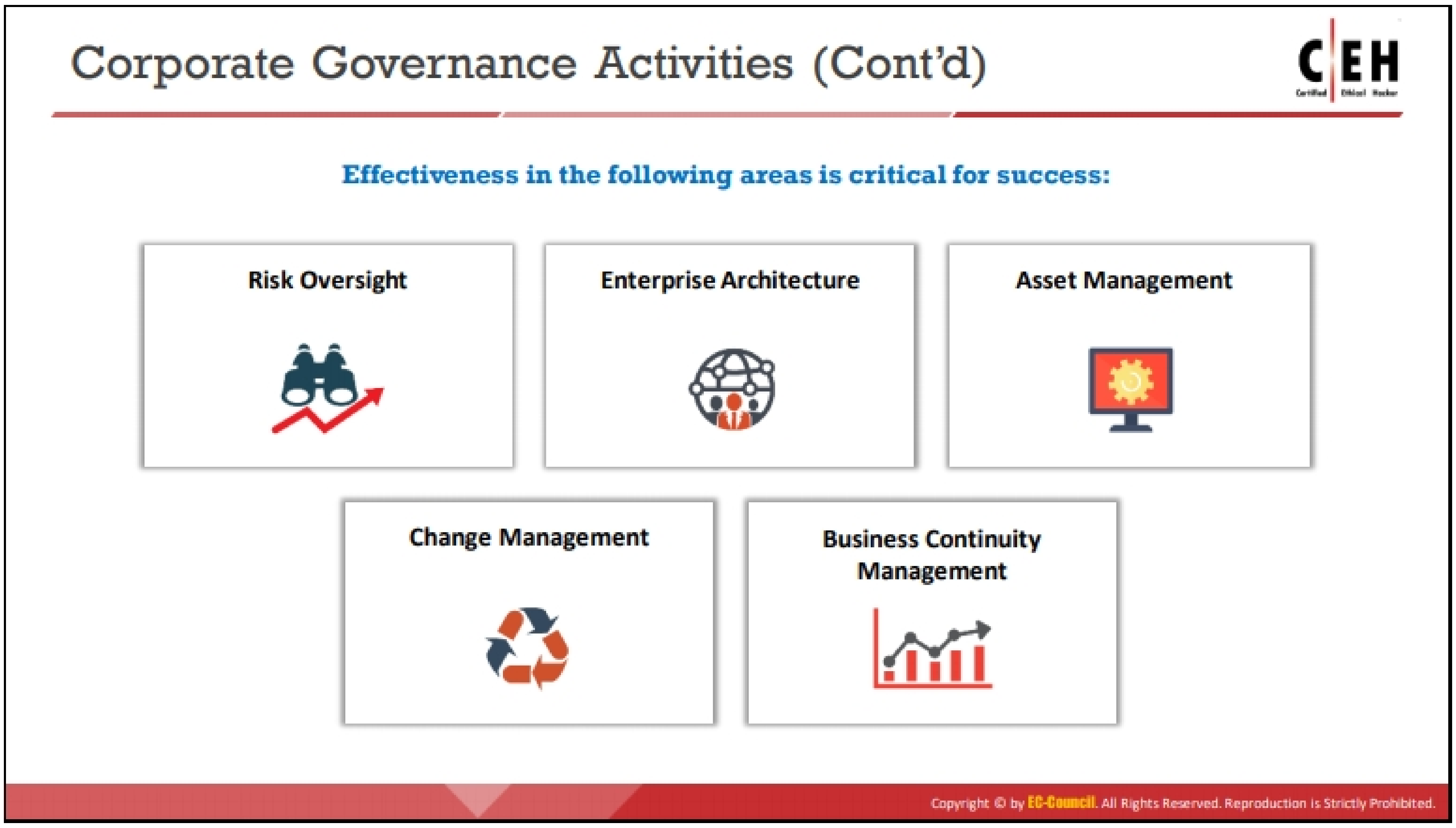


Corporate Governance Activities

Corporate Governance

- **IT Governance**
- **Information Security Governance**
- **Financial Governance**
- **Project Governance**

Corporate governance defines the framework of rules and practices by which a board of directors ensures accountability, fairness, and transparency in an organization's relationship with all its stakeholders

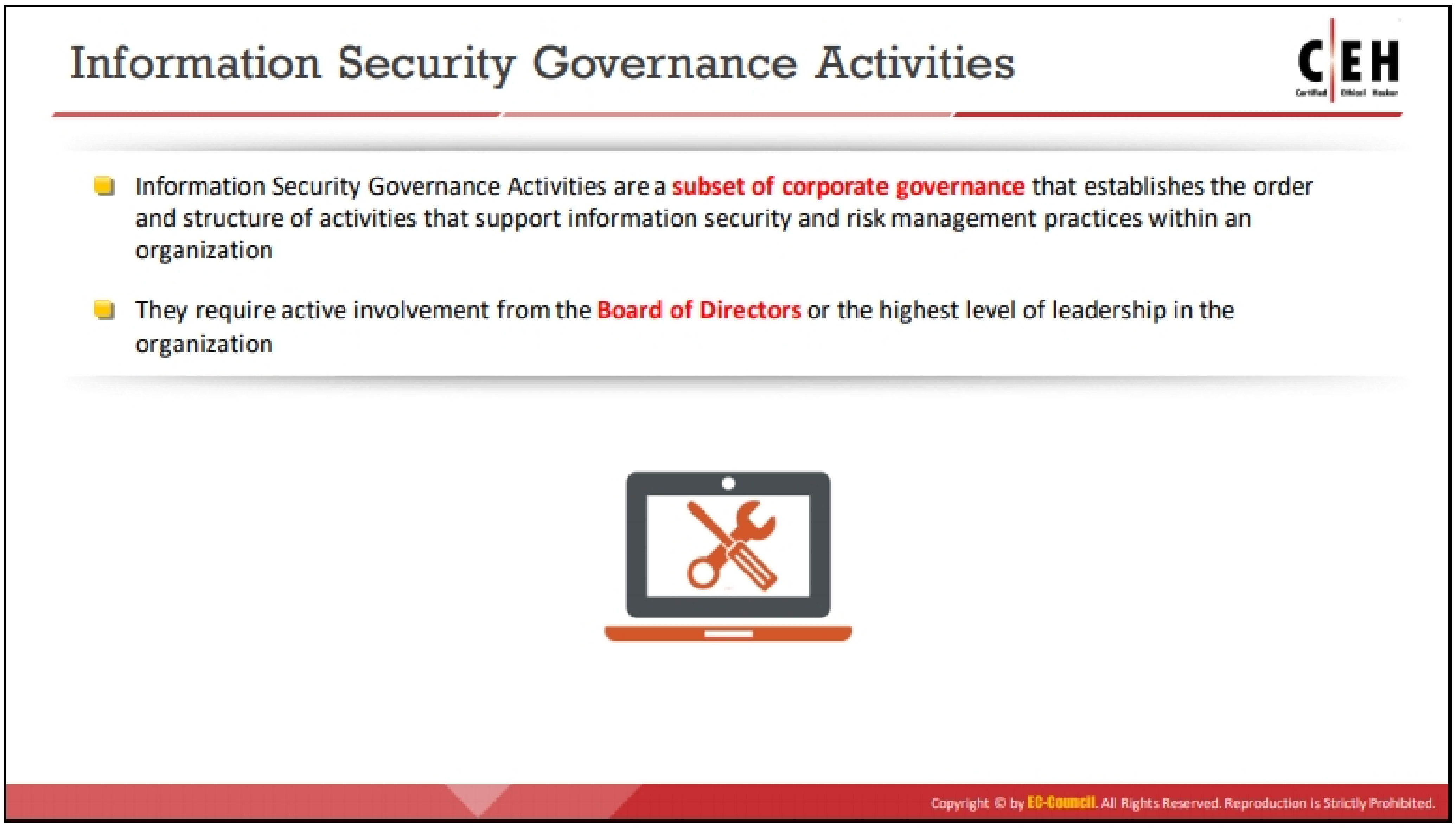


Corporate Governance Activities (Cont'd)

Effectiveness in the following areas is critical for success:

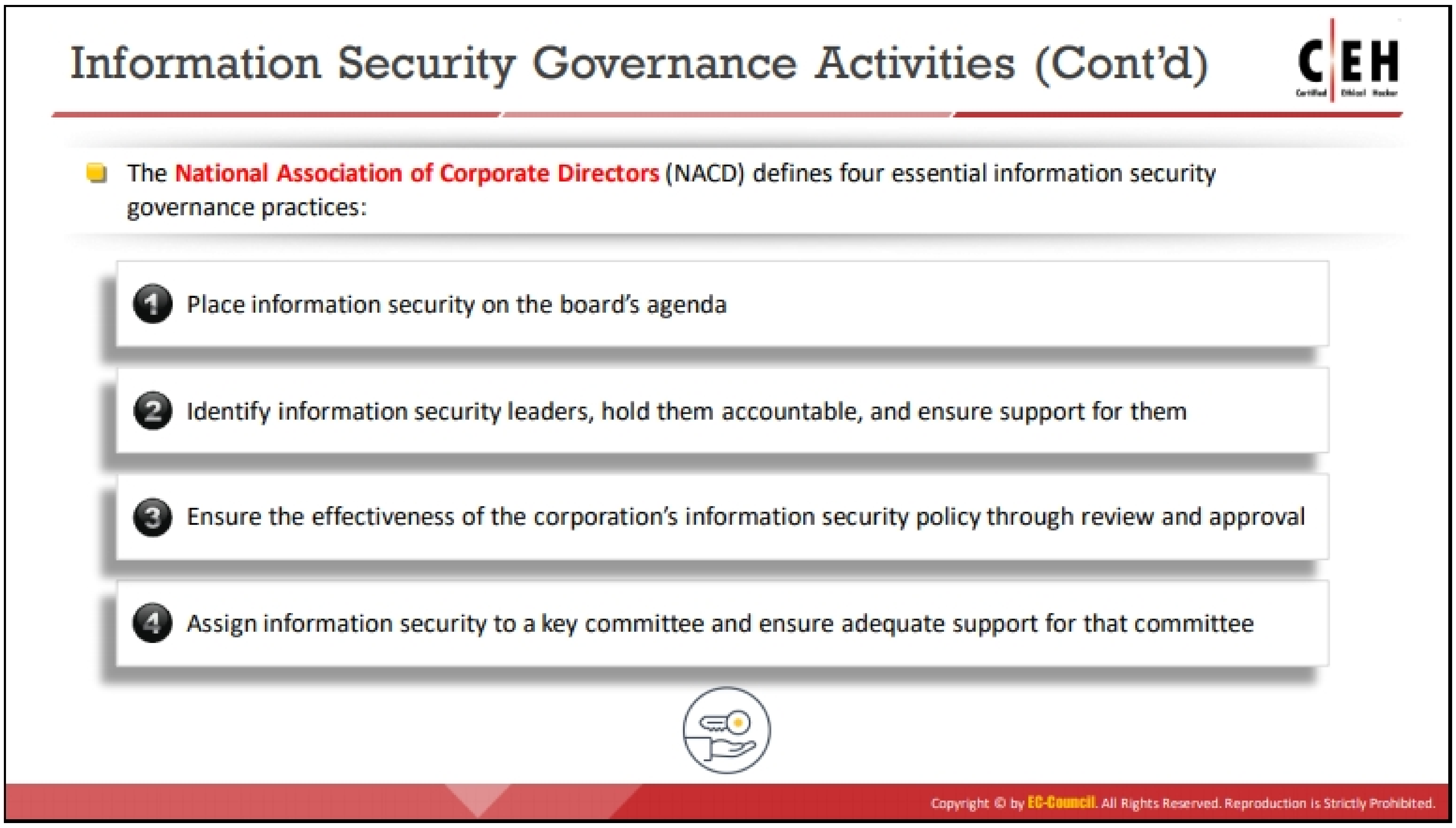
- **Risk Oversight**
- **Enterprise Architecture**
- **Asset Management**
- **Change Management**
- **Business Continuity Management**

Notes:



Information Security Governance Activities

- Information Security Governance Activities are a **subset of corporate governance** that establishes the order and structure of activities that support information security and risk management practices within an organization
- They require active involvement from the **Board of Directors** or the highest level of leadership in the organization

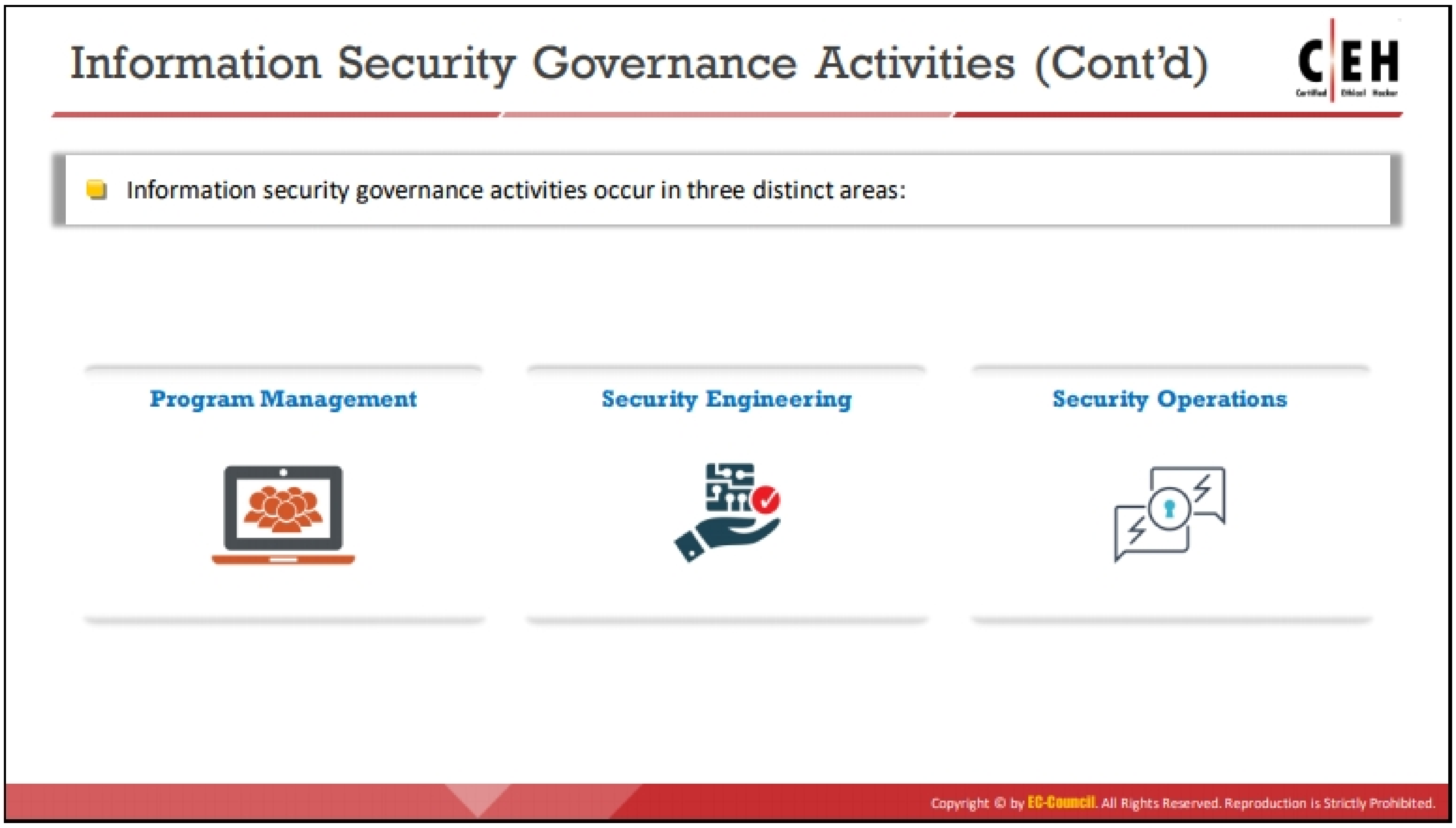


Information Security Governance Activities (Cont'd)

- The **National Association of Corporate Directors** (NACD) defines four essential information security governance practices:

1. Place information security on the board's agenda
2. Identify information security leaders, hold them accountable, and ensure support for them
3. Ensure the effectiveness of the corporation's information security policy through review and approval
4. Assign information security to a key committee and ensure adequate support for that committee

Notes: ______________________________



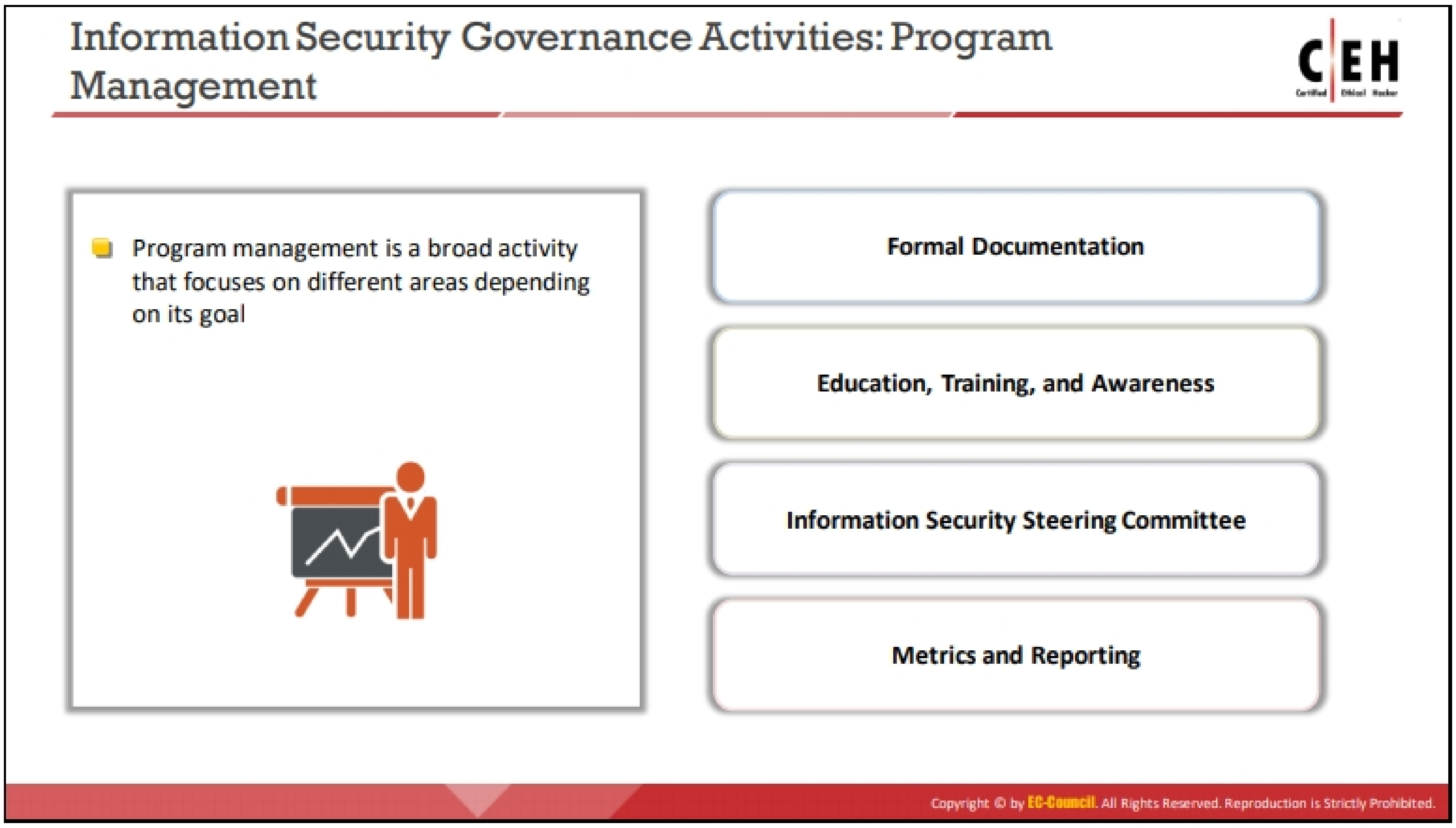
Information Security Governance Activities (Cont'd)

- Information security governance activities occur in three distinct areas:

Program Management

Security Engineering

Security Operations



Information Security Governance Activities: Program Management

- Program management is a broad activity that focuses on different areas depending on its goal

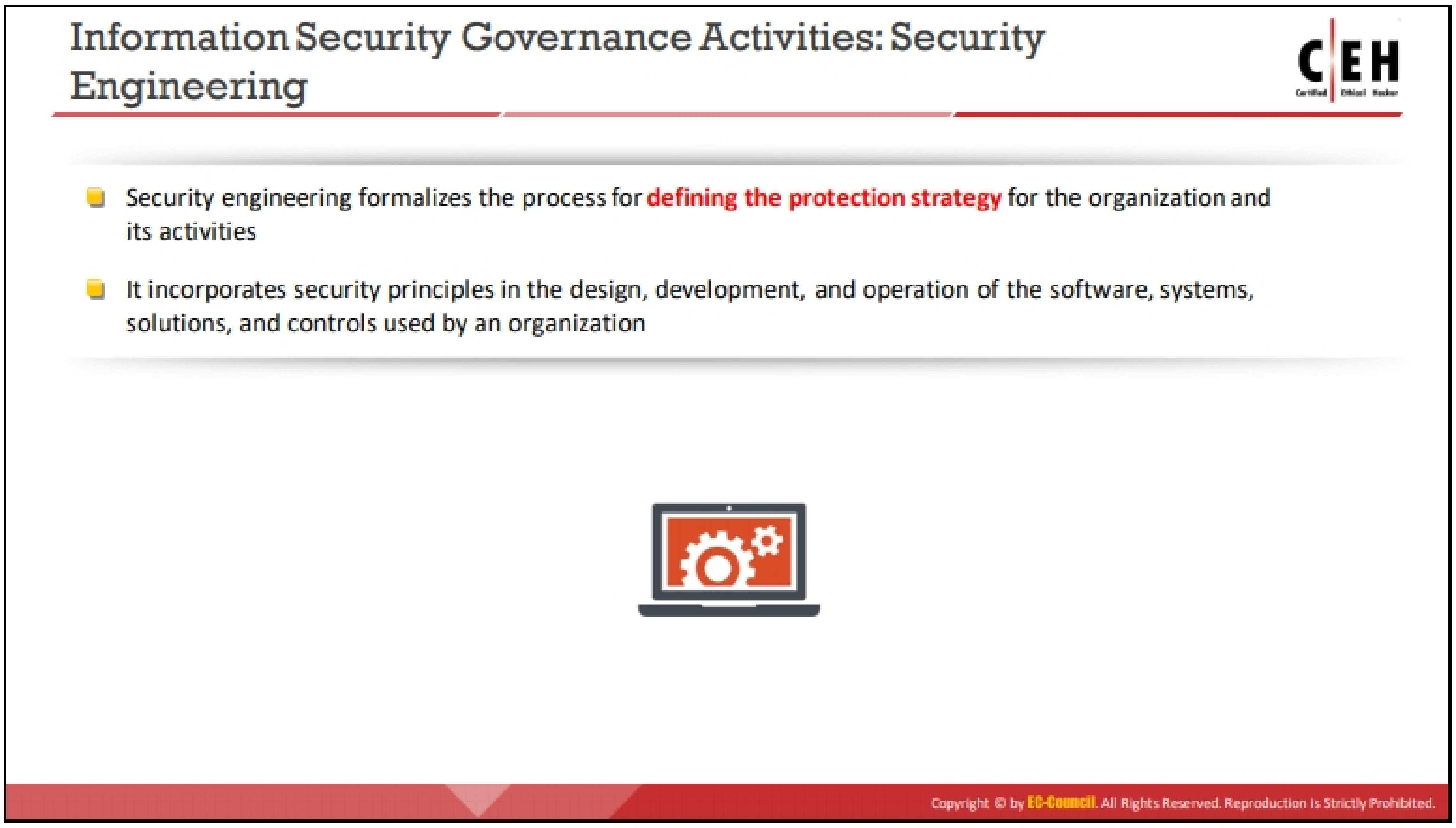
Formal Documentation

Education, Training, and Awareness

Information Security Steering Committee

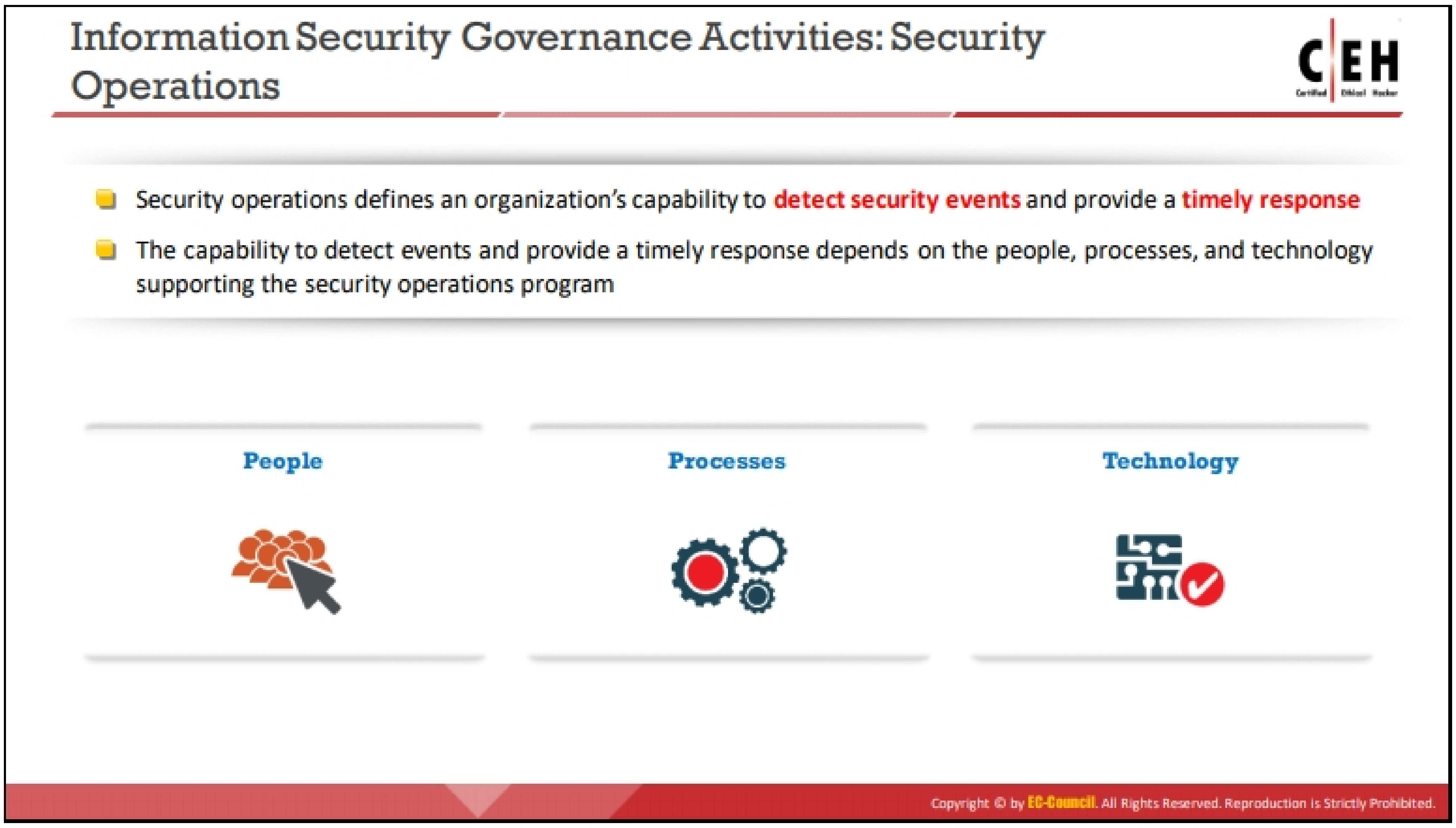
Metrics and Reporting

Notes:



Information Security Governance Activities: Security Engineering

- Security engineering formalizes the process for **defining the protection strategy** for the organization and its activities
- It incorporates security principles in the design, development, and operation of the software, systems, solutions, and controls used by an organization



Information Security Governance Activities: Security Operations

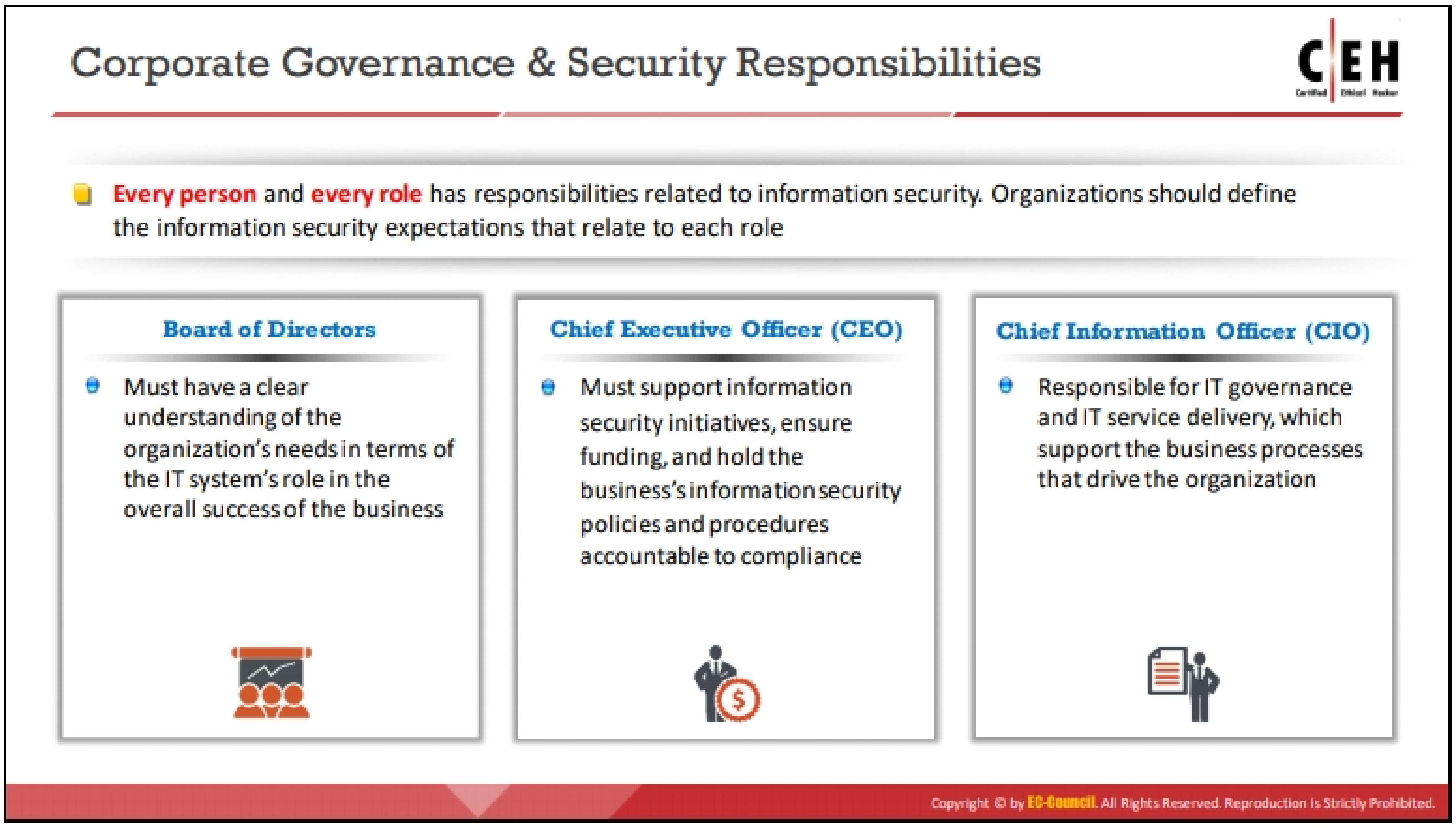
- Security operations defines an organization's capability to **detect security events** and provide a **timely response**
- The capability to detect events and provide a timely response depends on the people, processes, and technology supporting the security operations program

People

Processes

Technology

Notes:



Corporate Governance & Security Responsibilities

- Every person and every role has responsibilities related to information security. Organizations should define the information security expectations that relate to each role

Board of Directors

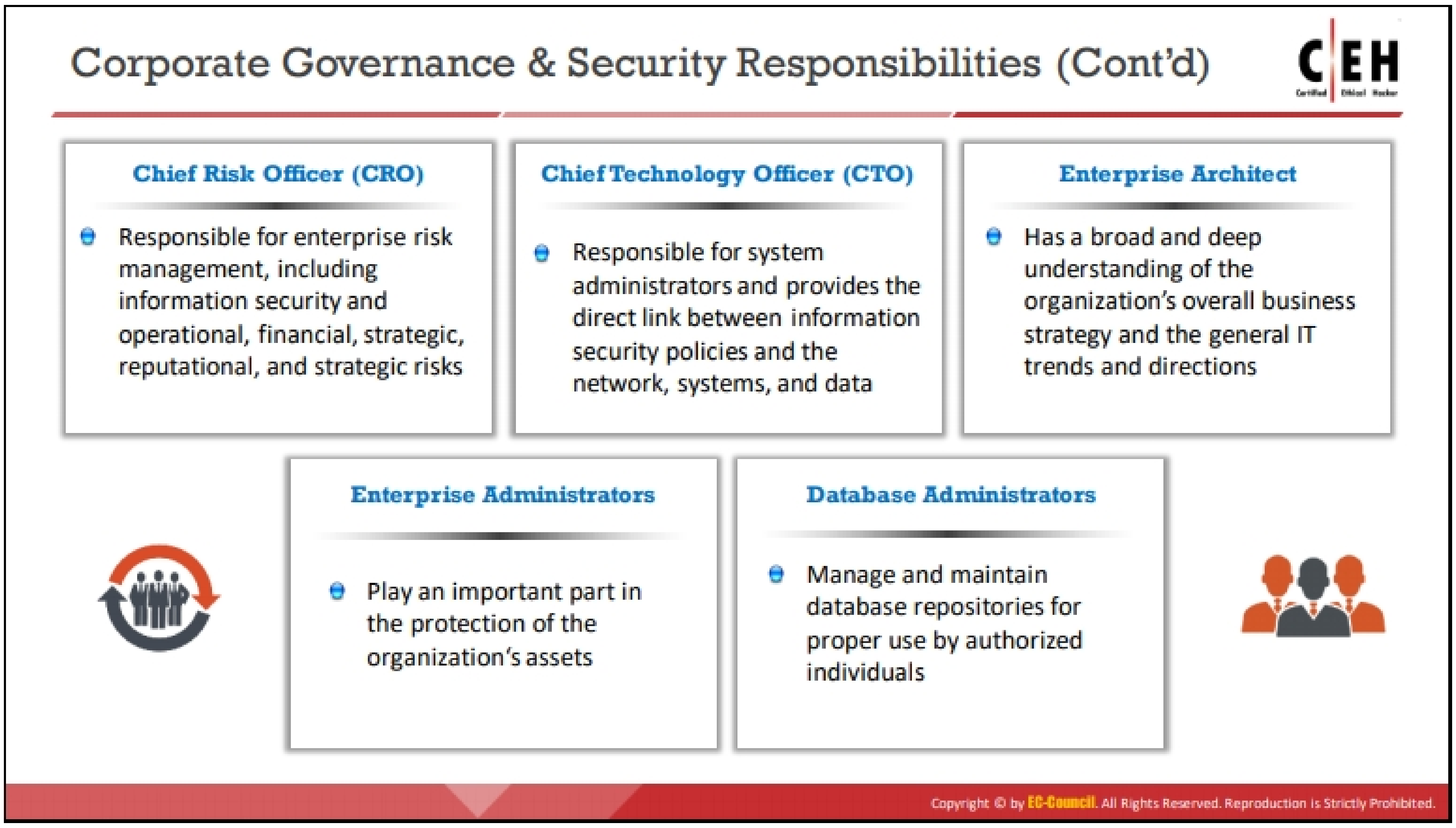
- Must have a clear understanding of the organization's needs in terms of the IT system's role in the overall success of the business

Chief Executive Officer (CEO)

- Must support information security initiatives, ensure funding, and hold the business's information security policies and procedures accountable to compliance

Chief Information Officer (CIO)

- Responsible for IT governance and IT service delivery, which support the business processes that drive the organization



Corporate Governance & Security Responsibilities (Cont'd)

Chief Risk Officer (CRO)

- Responsible for enterprise risk management, including information security and operational, financial, strategic, reputational, and strategic risks

Chief Technology Officer (CTO)

- Responsible for system administrators and provides the direct link between information security policies and the network, systems, and data

Enterprise Architect

- Has a broad and deep understanding of the organization's overall business strategy and the general IT trends and directions

Enterprise Administrators

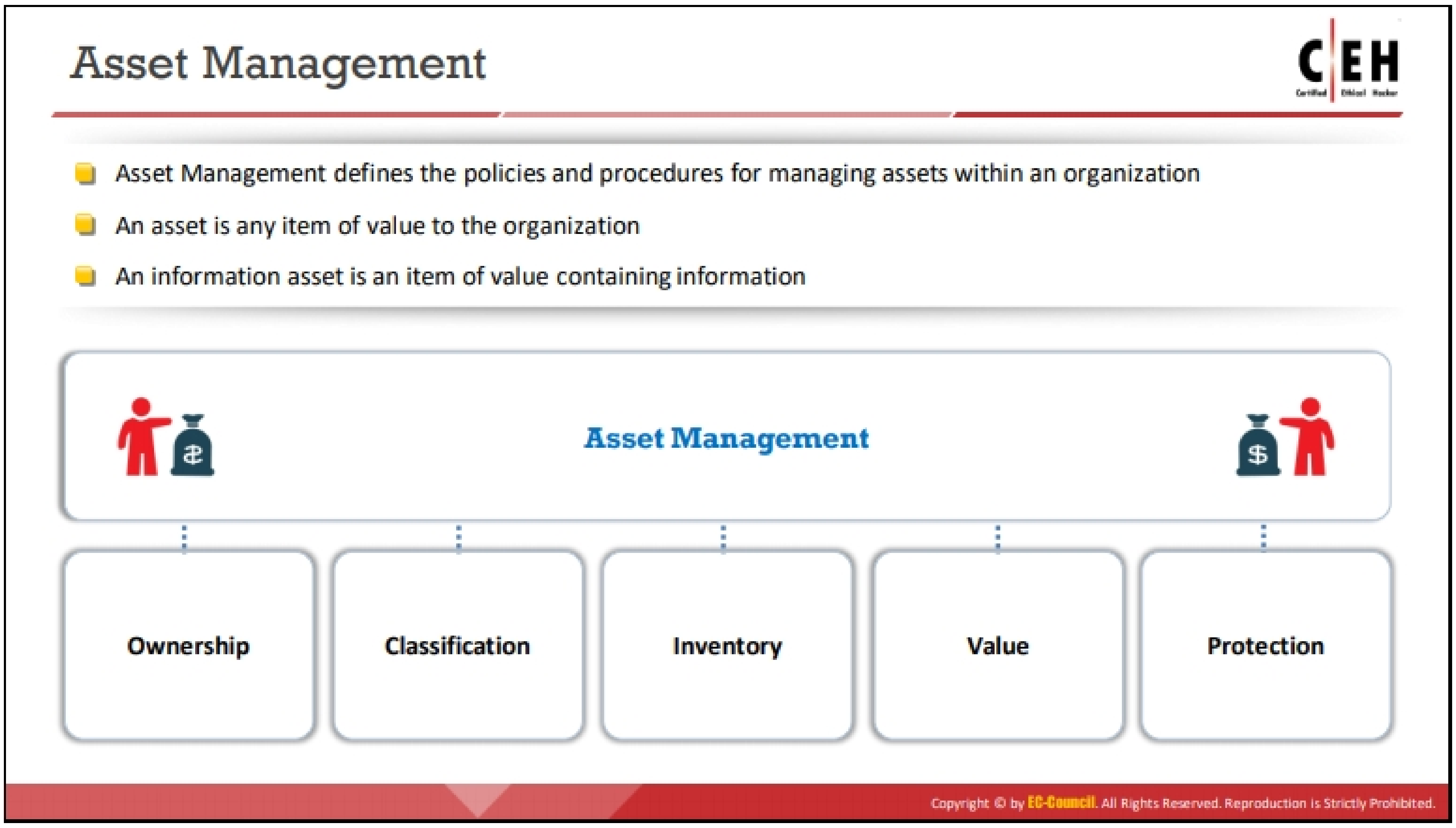
- Play an important part in the protection of the organization's assets

Database Administrators

- Manage and maintain database repositories for proper use by authorized individuals

Notes: ____________________

Asset Management and Security



Asset Management

- Asset Management defines the policies and procedures for managing assets within an organization
- An asset is any item of value to the organization
- An information asset is an item of value containing information

Asset Management

- **Ownership**
- **Classification**
- **Inventory**
- **Value**
- **Protection**

Notes: ____

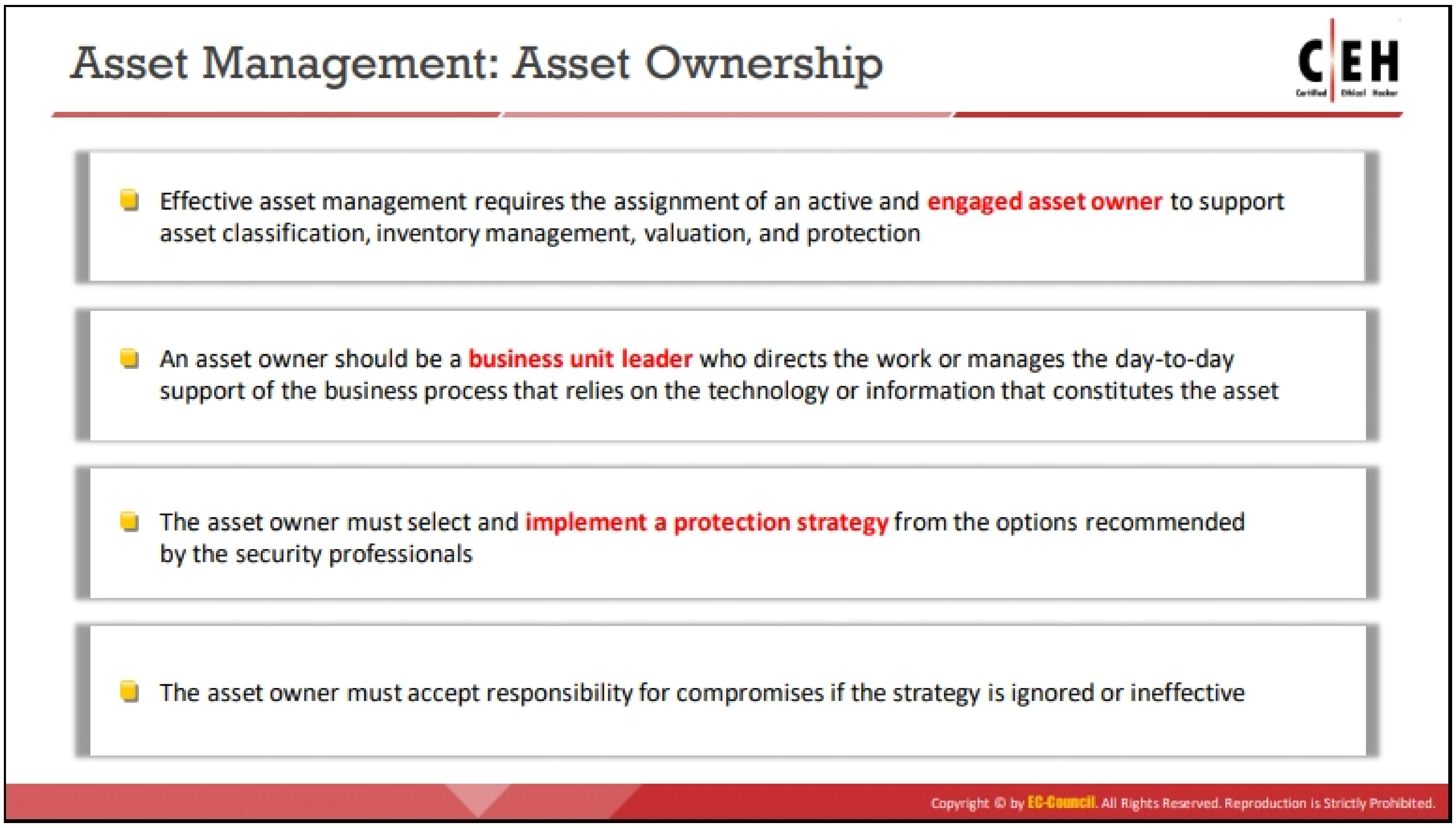
____

____

____

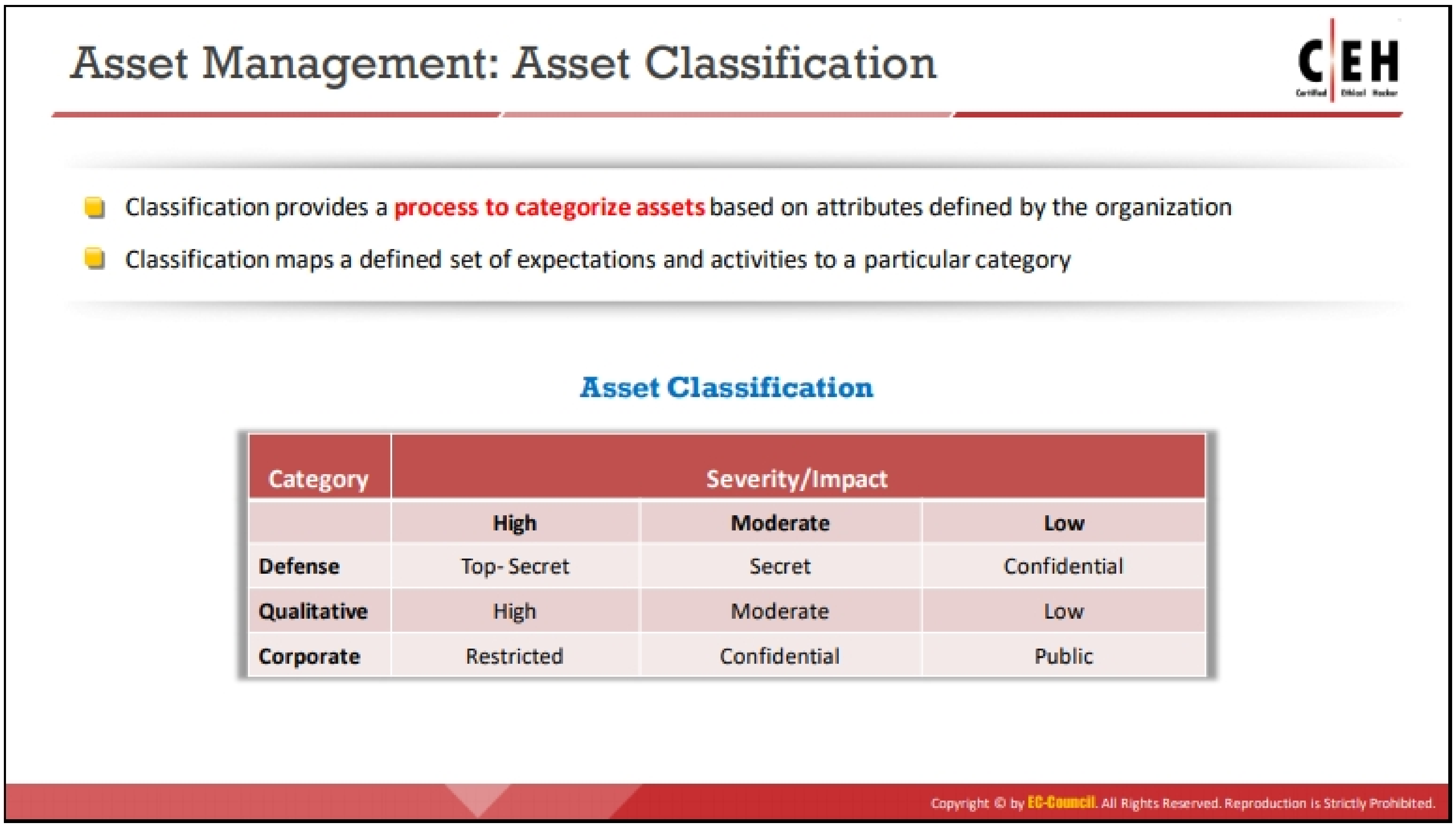
____

____



Asset Management: Asset Ownership

- Effective asset management requires the assignment of an active and **engaged asset owner** to support asset classification, inventory management, valuation, and protection
- An asset owner should be a **business unit leader** who directs the work or manages the day-to-day support of the business process that relies on the technology or information that constitutes the asset
- The asset owner must select and **implement a protection strategy** from the options recommended by the security professionals
- The asset owner must accept responsibility for compromises if the strategy is ignored or ineffective



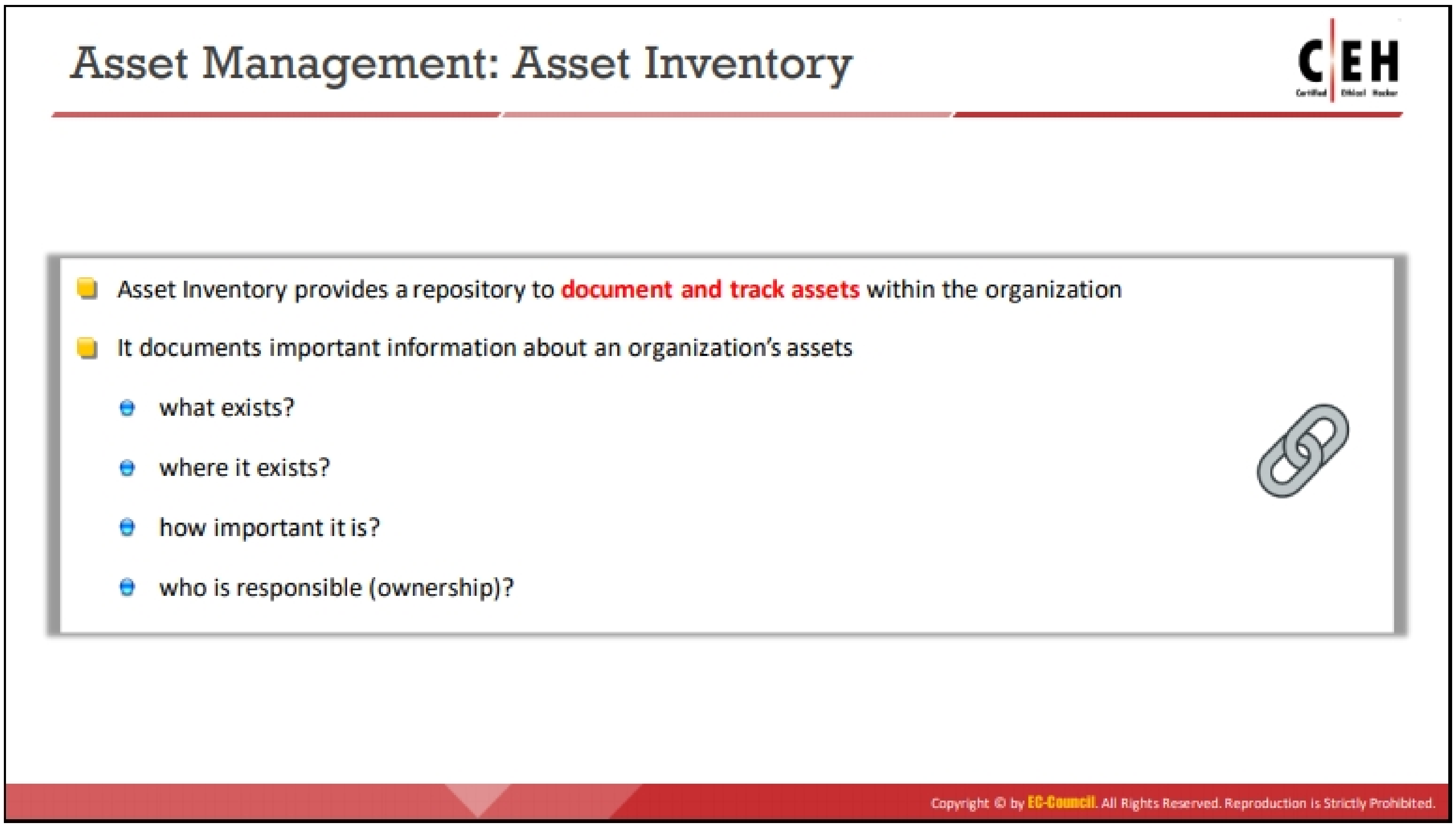
Asset Management: Asset Classification

- Classification provides a **process to categorize assets** based on attributes defined by the organization
- Classification maps a defined set of expectations and activities to a particular category

Asset Classification

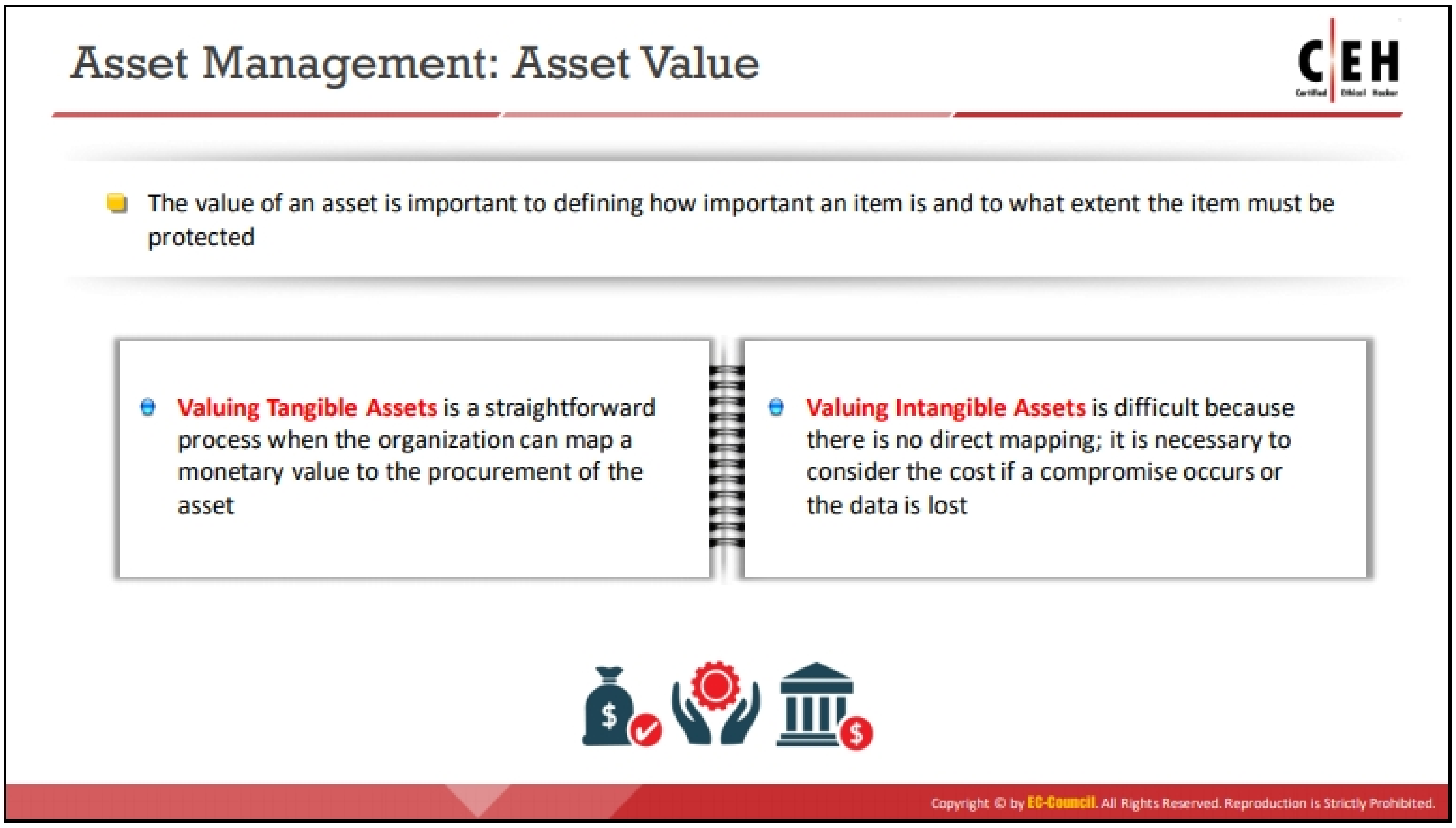
Category	Severity/Impact		
	High	**Moderate**	**Low**
Defense	Top- Secret	Secret	Confidential
Qualitative	High	Moderate	Low
Corporate	Restricted	Confidential	Public

Notes:



Asset Management: Asset Inventory

- Asset Inventory provides a repository to **document and track assets** within the organization
- It documents important information about an organization's assets
  - what exists?
  - where it exists?
  - how important it is?
  - who is responsible (ownership)?



Asset Management: Asset Value

- The value of an asset is important to defining how important an item is and to what extent the item must be protected

- **Valuing Tangible Assets** is a straightforward process when the organization can map a monetary value to the procurement of the asset

- **Valuing Intangible Assets** is difficult because there is no direct mapping; it is necessary to consider the cost if a compromise occurs or the data is lost

Notes: ____

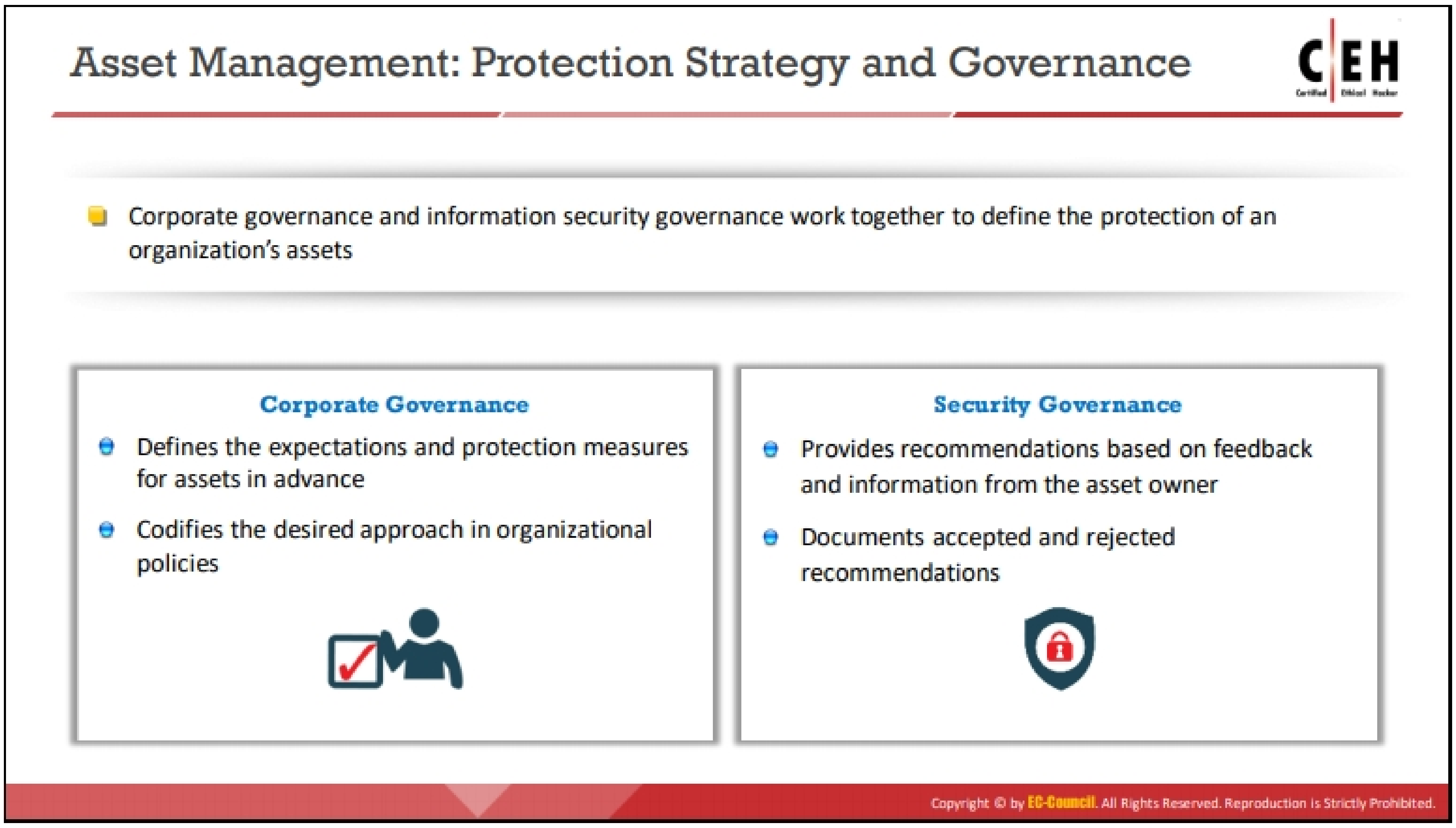
____

____

____

____

____



Asset Management: Protection Strategy and Governance

- Corporate governance and information security governance work together to define the protection of an organization's assets

Corporate Governance

- Defines the expectations and protection measures for assets in advance
- Codifies the desired approach in organizational policies

Security Governance

- Provides recommendations based on feedback and information from the asset owner
- Documents accepted and rejected recommendations

Notes: ____